JSP 440
D Def Sy/6/3

The Defence Manual of Security
Volumes 1, 2 and 3
Issue 2

MINISTRY OF DEFENCE
October 2001

By Command of the Defence Council

This page intentionally left blank.

JSP 440 THE DEFENCE MANUAL OF SECURITY: ISSUE 2

1. This manual comprises the following parts of JSP 440, the Defence Manual of Security:

a. Issue 2 of Volume 1. The principles of protective security, the responsibilities of those concerned with applying them, and physical security policy.

b. Issue 2 AL 1[1] of Volume 2. Personnel security policy including the vetting system, line manager responsibility and travel security.

c. Issue 2 of Volume 3. Guidance and policy on the security of Communications and Information Systems (CIS).

2. The three volumes have been updated to reflect the organisational changes of the Security Structures Review (see Volume 1 Chapter 2 for further details), and in the case of Volume 2 the collocation of the Defence Vetting Agency at York. Issue 2 also incorporates a number of amendments to JSP 440 that have been issued to security staffs in the form of policy letters or separate security instructions.

3. These three volumes can be viewed on the MODWeb (http:/www.chots.mod.uk/admin_instructions/security/security.htm) and on connected MOD and single Service intranets. They are available on CD ROM for establishments that are not able to access the MODWeb and connected intranets. A limited number of hard copies of Issue 2 are being published, as requested by the Royal Navy and Army. Those using the hard copy version are warned that there will inevitably be a delay between the electronic publication of Issue 2, and publication in hard copy. This also applies to future amendments to Issue 2.

4. The publication of Issue 2 of JSP 440 represents the first step towards production of security policy guidance that will fully reflect the principles of delegated security risk management set out in the Security Structures Review. The rewrite of JSP 440 will be designated 'Issue 3 JSP 440'. Issue 3 JSP 440 is not expected to be published (in electronic form) until 2003. In the meantime, interim guidance will be issued in the form of DSO Guidance Notes and Issue 2 will also be amended approximately at six-monthly intervals. The first four DSO Guidance Notes are included on the Issue 2 CD ROM; they are also published separately on MODWeb and are being placed in the Army Electronic Library.

5. Establishments and units should address any requests for further advice or interpretation in the first instance to their TLB Principal Security Adviser (see Volume 1 Chapter 2 for details). Should they wish to seek advice from Directorate of Defence Security staff, the following are the desk – level points of contact:

[1] The original Issue 2 of Volume 2 was published during 2000 before the Security Structures Review was completed.

Volume 1 Protective Security	Volume 2 Personnel Security	Volume 3 IT Security
PhysSy(Gd/ROE)	Pers Sy 2	Hd InfoSy(Pol)
Tel: 020 721 80289 CHOtS: DDefSy- Phys(Gd/ROE)	Tel: 020 721 83764 CHOtS: DDefSy- Pers Sy 2	Tel: 020 721 83746 CHOtS: DDefSy- Hd InfoSy(Pol)

6. Suggestions for amendments to and comments on the Defence Manual of Security should be sent through TLB and Trading Fund Principal Security Advisers to the Directorate of Defence Security.

7. Requests for additional copies of the CD ROM should be sent to:

DSDC(L)6a2
Defence Storage and Distribution Centre
Mwrwg Road
Llangennech
Llanelli
South Wales
SA14 8YP

John Cochrane

J C COCHRANE
Director Defence Security

26 October 2001

VOLUME 1
Issue 2

PROTECTIVE SECURITY

MINISTRY OF DEFENCE
October 2001

This page intentionally left blank.

VOLUME 1 – PROTECTIVE SECURITY

CONTENTS

Chapter

CHAPTER 1

PRINCIPLES OF SECURITY

This page intentionally left blank

CHAPTER 1

PRINCIPLES OF SECURITY

The Definition of Protective Security

0101. Protective security is the protection of assets from compromise. Compromise can be a breach of:

a. **Confidentiality.** The restriction of information and other valuable assets to authorized individuals (e.g. protection from espionage, eavesdropping, leaks and computer hacking).

b. **Integrity**. The maintenance of information systems of all kinds and physical assets in their complete and usable form (e.g. protection from unauthorized alteration to a computer programme).

c. **Availability**. The permitting of continuous or timely access to information systems or physical assets by authorized users (e.g. protection from sabotage, malicious damage, theft, fire and flood).

0102. In assessing integrity and availability, consideration must be given to both the **direct** and **indirect** consequences of compromise. For example, the theft of a personal computer may be of limited **direct** consequence as such equipment can be relatively cheaply replaced. The loss of the information contained on the computer may have significant **indirect** consequences, particularly if no arrangements have been made for backup storage of the information it contains.

The Security System

0103. Assets are defined as "anything of value, either tangible or intangible that is owned or used by an organization or business". They can be documents and information; material such as buildings, equipment, valuables or cash; operating systems or personnel. Material assets can have different degrees of value, these are defined within the following protective markings:

a. **TOP SECRET**. The compromise of TOP SECRET information or material would be likely to threaten directly the internal stability of the UK or friendly countries; to lead directly to widespread loss of life; to cause exceptionally grave damage to the effectiveness or security of UK or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations; to cause exceptionally grave damage to relations with friendly governments; to cause severe long-term damage to the UK economy.

b. **SECRET**. The compromise of SECRET information or material would be likely: to raise international tension; to damage seriously relations with friendly governments; to threaten life directly, or seriously prejudice public order, or individual security or liberty; to cause serious damage to the operational effectiveness or security of UK or allied forces or the continuing effectiveness of highly valuable security or intelligence operations; to cause substantial material damage to national finances or economic and commercial interests.

c. **CONFIDENTIAL**. The compromise of CONFIDENTIAL information or material would be likely to materially damage diplomatic relations (i.e. cause formal protest or other sanction); to prejudice individual security or liberty; to cause damage to the operational effectiveness or security of UK or allied forces or the effectiveness of valuable security or intelligence operations; to work substantially against national finances or economic and commercial interests; substantially to undermine the financial viability of major organizations; to impede the investigation or facilitate the commission of serious crime; to impede seriously the development or operation of major government policies; to shut down or otherwise substantially disrupt significant national operations.

d. **RESTRICTED**. The compromise of RESTRICTED information or material would be likely to affect diplomatic relations adversely; to cause substantial distress to individuals; to make it more difficult to maintain the operational effectiveness or security of UK or allied forces; to cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or companies; to prejudice the investigation or facilitate the commission of crime; to breach proper undertakings to maintain the confidence of information provided by third parties; to impede the effective development or operation of government policies; to breach statutory restrictions on disclosure of information; to disadvantage government in commercial or policy negotiations with others; to undermine the proper management of the public sector and its operations.

0104. When an asset merits a protective marking the appropriate levels of protection shown at Annex A are to be provided. The protective marking given to a document must be determined solely on the information it contains. It is therefore very important that the protective marking selected is correct.

Special Markings

0105. Only those with a need to know, or need to hold, should have access to protectively marked information. When it is necessary to provide additional protection by reinforcing the "need to know" principle, special markings that restrict

access should be used, normally in conjunction with a protective marking. Special markings consist of:

a. **National Caveats.** National caveats exist for the additional protection of certain types of protectively marked UK material, e.g. UK EYES ONLY and CANUKUS EYES ONLY. Definitions of these and other caveats, and advice on their use, are given in Chapter 16.

b. **Descriptors.** Descriptors help to implement the "need to know" principle by indicating the nature of the asset's sensitivity and the need to limit access accordingly. A list of MOD descriptors is at Annex B.

c. **Additional Markings.** Additional markings may be required to ensure the special handling of some material to indicate particular aspects of ownership, issue or release, e.g. CODEWORD material. Further details are in Chapter 4.

d. **International Defence Organization (IDO) Markings.** IDOs e.g. the North Atlantic Treaty Organization (NATO) and the Western European Union (WEU) and their member nations, use similar protective markings to the UK prefixed NATO or WEU as appropriate. Further details are in Chapter 4.

The Threat

0106. The following paragraphs detail the five threats to security.

Espionage

0107. Espionage is defined as "Attempts to acquire information covertly or illegally in order to assist a foreign power". Foreign intelligence services are continuously collecting information for intelligence purposes. They:

a. Work mainly through agents who are either introduced into a country or recruited locally. Such agents in their search for targets may be expected to seek out those with human weaknesses who can be exploited particularly through corruption or blackmail.

b. Mount technical operations such as eavesdropping, including telephone interception, interception of radio communications (SIGINT) and surveillance.

No establishment is immune from attack. No one with access or potential access to protected assets is too unimportant to be cultivated either as a useful contact or

possible agent. Definitions of levels of espionage threat, including from SIGINT and extremists, are at Annex C.

Sabotage

0108. Sabotage is defined as "An act falling short of a military operation, or an omission, intended to cause physical damage in order to assist a hostile foreign power or to further a subversive political aim". The following should be noted:

a. Although sabotage on a major scale is likely only in the period immediately before or after the outbreak of war, it can be used as a means of advancing political causes.

b. In peacetime agents of foreign intelligence services may select targets for future attack by trained, experienced saboteurs.

c. Saboteurs may be capable of using highly sophisticated methods and their aim will be to disrupt essential communications, damage vital military installations, impede industrial production and lower national morale.

d. In acts of terrorism, sabotage may be used for widely differing purposes ranging from attacking unimportant targets with the object of attracting publicity to the terrorists' cause, to damaging important installations as part of a major terrorist campaign.

Subversion

0109. Subversion is defined as "Action designed to weaken the military, economic or political strength of a nation by undermining the morale, loyalty or reliability of its citizens". The threat from subversion stems not only from foreign intelligence services but also from members of organizations such as those based on anarchism, religious fanaticism, and extreme left and right wing ideologies. Organizations with these ideologies may try to acquire protectively marked information, not necessarily to give to a potential enemy, but to use it in a way that would bring the government in general into disrepute.

Terrorism

0110. Terrorism is defined as "The unlawful use or threatened use of force or violence against individuals or property in an attempt to coerce or intimidate governments or societies to achieve political, religious or ideological objectives". It represents a world-wide threat and is characterized by sudden and violent attacks. Terrorist methods include murder, kidnapping, hostage-taking, hijacking of air, sea, road and rail transport, and attacks on people, buildings, aircraft and vehicles by

small arms, mortars, bombs and mines. Definitions of terrorist threat levels are at Annex D. See also Chapter 7.

Non Traditional Threats Posed by Other Individuals or Organizations

0111. Government assets are under threat from a variety of sources beyond those traditionally regarded as hostile or otherwise of significance in terms of national security. The responsibility for providing advice to counter non-traditional threats will not always lie with the security staff and may often be provided by the appropriate Service, MOD or civil police agency. The main threats of this type are posed by investigative journalists, pressure groups, investigation agencies, criminal elements, disaffected staff, dishonest staff and computer hackers. The types of threat from these sources can be categorized in six broad groups:

a. **Confidentiality**. Compromise of politically sensitive information. This threat is presented by:

(1) Pressure groups and investigative journalists attempting to obtain sensitive information.

(2) Unauthorized disclosure of official information (leaks).

b. **Exploitation of Sensitive Information.** Debt collection agencies and investigation agencies are known to attempt to obtain personal information held in confidence by government. Investigative journalists have exploited personal tax information; they also target commercial and financial information as do criminal elements seeking financial advantage.

c. **Theft, Burglary and Fraud.** There is a growing threat of theft, particularly of IT equipment. Arms, ammunition and explosives are always at particular risk. Theft may occur through burglary or the actions of dishonest staff. Establishments responsible for the collection or disbursement of public funds are prone to fraud and there is an increasing threat of fraud through the manipulation of IT systems.

d. **Corruption, Destruction, or Unauthorized Access to, Computer Data.** The integrity of data held on computer systems is under threat mainly from disaffected staff. Existing levels of programming expertise, the ready availability of malicious software, e.g. viruses, and the ease with which they can be deliberately or accidentally introduced, combine to create a substantial threat. It is apparent that some staff misguidedly interfere with or compromise systems. There is also a level of threat of damage resulting from

the actions of hackers - either those with legitimate access to systems or those without such access.

e. **Pressure Groups.** Pressure groups for such causes as animal rights, nuclear disarmament and the environment will sometimes carry out demonstrations against MOD policy and activities. Although often confined to peaceful demonstrations, extremist elements can cause violent attacks on individuals and property, which can pose a threat as significant as terrorism.

f. **Criminal Damage.** Employees, dependants, visitors or intruders can carry out criminal damage.

g. **Natural Disaster.** Natural disasters are risks to the integrity or availability of facilities, buildings or equipment etc caused by such incidents as fire, flooding, subsidence, or lightning strike.

Components of Security

0112. There are two different and interdependent parts of security:

a. **Security Intelligence.** The collection of information and production of intelligence concerning the security threat. Plans to counter the activities of foreign intelligence services or subversive organizations and individuals must be based on accurate and timely intelligence concerning the identity, capabilities and intentions of the hostile elements. This intelligence is known as 'security intelligence'. It is derived from studying attempts to break through security controls, combined with knowledge gained from penetrating hostile organizations. One means of obtaining security intelligence is the investigation of breaches of security. Although security intelligence is a matter which is principally the concern of security staffs and security units, all personnel in the MOD, whether Service or civilian, contribute to it by the prompt reporting of suspicious activity.

b. **Protective Security** - consists of:

(1) **Laws, Orders and Instructions**. These measures range from the Official Secrets Acts to Establishment Security Standing Orders.

(2) **Physical Measures**. Physical measures are the physical obstacles, which protect specific security interests. These range from perimeter defences such as fences and lighting to security containers.

(3) **Personnel Security Measures**. The aim of personnel security measures is to ensure that only reliable and trustworthy persons have access to protected information.

(4) **Security Education and Training**. The aim of security education is to ensure that all who work for the MOD, irrespective of access, understand both the threat and their general responsibilities for countering it. The aim of security training is to ensure that individuals who have specific security responsibilities as part of their normal employment are properly trained in their security duties. Security education and training is the responsibility of commanders and HOE at all levels.

(5) **Security Procedures**. Security procedures include document handling, control of access, checks and audits.

Risk

0113. Risk can be defined as "a future uncertain event" and is measured in terms of likelihood and impact. No amount of security measures can ever totally eliminate risk. The vulnerability of assets to threats must be reduced so that the likelihood of compromise or loss is reduced to an acceptable level. Over protection leads to a waste of resources and under protection leads to an unwarranted risk. Security measures selected must be balanced and cost effective in their application. Further details are in Chapter 3.

The Precepts of Security

0114. The main precepts of security are:

a. **Command Responsibility.** Whilst every individual who works for the MOD has a personal responsibility to promote and maintain security at all times, HOE are responsible for security within their establishments and commanders/heads of department have overall responsibility for security within their formations or departments.

b. **Need to Know.** Knowledge of protected matters must be limited strictly to those who are security cleared to the appropriate level and who need such knowledge in order to carry out their official duties.

c. **Need to Hold.** Protectively marked documents and material must only be retained by individuals who need them for the efficient discharge of their duties.

d. **Defence in Depth.** Effective protective security results from a carefully planned system of defensive security measures designed to protect information, material, personnel, activities and installations. These controls must form an interdependent and interlocking series of defences arranged in depth outward from the target. (A diagram is at Annex E).

e. **Make Sense.** Security measures must be practicable and cost effective.

ANNEX A TO CHAPTER 1

SECURITY STANDARDS

Assets in each level of the protective marking system are required to be protected to a specific level of protection. The protective markings therefore provide a means of establishing the value of, and hence the level of protection to be afforded to, particular assets. These levels of protection are detailed below.

TOP SECRET: Information and other assets should be held, processed, transmitted or transported and destroyed under conditions which ensure that only those who can be trusted with them and have been authorized gain access to them, that actual or attempted compromises will be detected, and those responsible will be identified.

SECRET: Information and other assets should be held, processed, transmitted or transported and destroyed under conditions which make it highly unlikely that anyone without authorized access will, by chance or design, gain access to them, that compromise will go undetected or that those responsible will remain unidentified.

CONFIDENTIAL: Information and other assets should be held, processed, transmitted or transported and destroyed under conditions which inhibit casual or wilful access by unauthorized people and which are likely to assist in the identification of compromises.

RESTRICTED: Information and other assets should be held, processed, transmitted or transported and destroyed with discretion in order to avoid access by unauthorized people.

This page intentionally left blank.

ANNEX B TO CHAPTER 1

DESCRIPTORS

1. Descriptors may be helpful in implementing the "need to know" principle by indicating the nature of the asset's sensitivity and thereby helping to ensure that access is limited accordingly. Aside from PERSONAL, which by definition requires that the information is only made available in the first instance to the addressee, the descriptors will normally be used in conjunction with a protective marking. Used alone, descriptors may indicate who should see the material but do not of themselves impose any particular handling or level of protection. A list of MOD descriptors is below:

a. **APPOINTMENTS.** Concerning actual or potential appointments that have not been announced.

b. **BUDGET.** Concerning proposed or actual measures for the budget before they are announced.

c. **COMMERCIAL.** Subject matter of actual or potential commercial value, the disclosure of which would prejudice a commercial interest. The rules for the use of this marking are given in Chapter 12.

d. **CONTRACTS.** Matters concerning tenders under consideration and the terms of tenders accepted.

e. **CONTROL (or DS).** Exercise papers for use only by control or directing staff.

f. **EXAMINATION.** Subject matter relating to setting, marking or future examination papers. (For MOD use only).

g. **EXERCISES.** Concerning orders and instructions pertaining to military exercise at home and abroad.

h. **HONOURS.** Matters concerning military or civilian honours and awards.

i. **INTELLIGENCE.** Concerning intelligence source material and assessments.

j. **INVESTIGATION.** Concerning investigations into disciplinary or criminal matters.

k. **LOCSEN.** Concerning locally sensitive information.

l. **MANAGEMENT.** Management policy and planning matters, the premature disclosure of which would not be in the interest of the Ministry of Defence or the Services.

m. **MEDICAL.** Medical matters concerning individuals including reports and records.

n. **OPERATIONS.** Concerning orders and instructions pertaining to military operations at home and abroad.

o. **PERSONAL.** Material only to be seen by the person to whom it is addressed.

p. **POLICE.** Police matters concerning police operations and activities.

q. **POLICY.** Concerning proposals for new or changed policy before publication.

r. **STAFF.** Matters concerning the administration (e.g. confidential reports), discipline, security status and service of named or identifiable personnel.

s. **VETTING.** Concerning matters pertaining to the security clearance of personnel.

t. **VISITS.** Concerning details of visits by, for example, royalty, ministers or very senior staff.

2. Should additions to this list be sought, they should be addressed to D Def Sy through the security reporting chain.

ANNEX C TO CHAPTER 1

DEFINITIONS OF LEVELS OF ESPIONAGE THREAT

The definitions and threat levels below are used by the Security Service when considering the threat from espionage, including SIGINT and Extremist threats.

Grade	Definition
VERY HIGH	Intelligence shows that attacks against this target or the UK's interests in this location are a top priority for an individual, group or country that has a formidable degree of capability and effectiveness.
HIGH	Intelligence shows that attacks against this target or the UK's interests in this location are an important priority for an individual, group or country, which is capable and effective.
SIGNIFICANT	Intelligence indicates that attacks against this target or the UK's interests in this location are high priority for an individual, group or country that has limited capability or effectiveness. or Intelligence indicates that attacks against this target or the UK's interests in this location are a medium priority for an individual, group or country, which is capable and effective.
MODERATE	Intelligence indicates that attacks against this target or the UK's interests in this location are a medium priority for an individual, group or country, which has a limited degree of capability and effectiveness.
LOW	Intelligence indicates that attacks against this target or the UK's interests in this location are an unimportant priority for an individual, group or country, which has little capability.
NEGLIGIBLE	Intelligence indicates that attacks against this target or the UK's interests in this location are unlikely to be considered by an individual, group or country; or Intelligence indicates that an individual, group or country lacks both capability and effectiveness.

This page intentionally left blank.

ANNEX D TO CHAPTER 1

DEFINITIONS FOR LEVELS OF TERRORIST THREAT

1. The definitions and terms for use in terrorist threat assessments have been agreed by ACPO for use by the civil police and national agencies.

2. These standard definitions are to be used by all those concerned in assessing the terrorist threat and implementing counter-measures in the MOD.

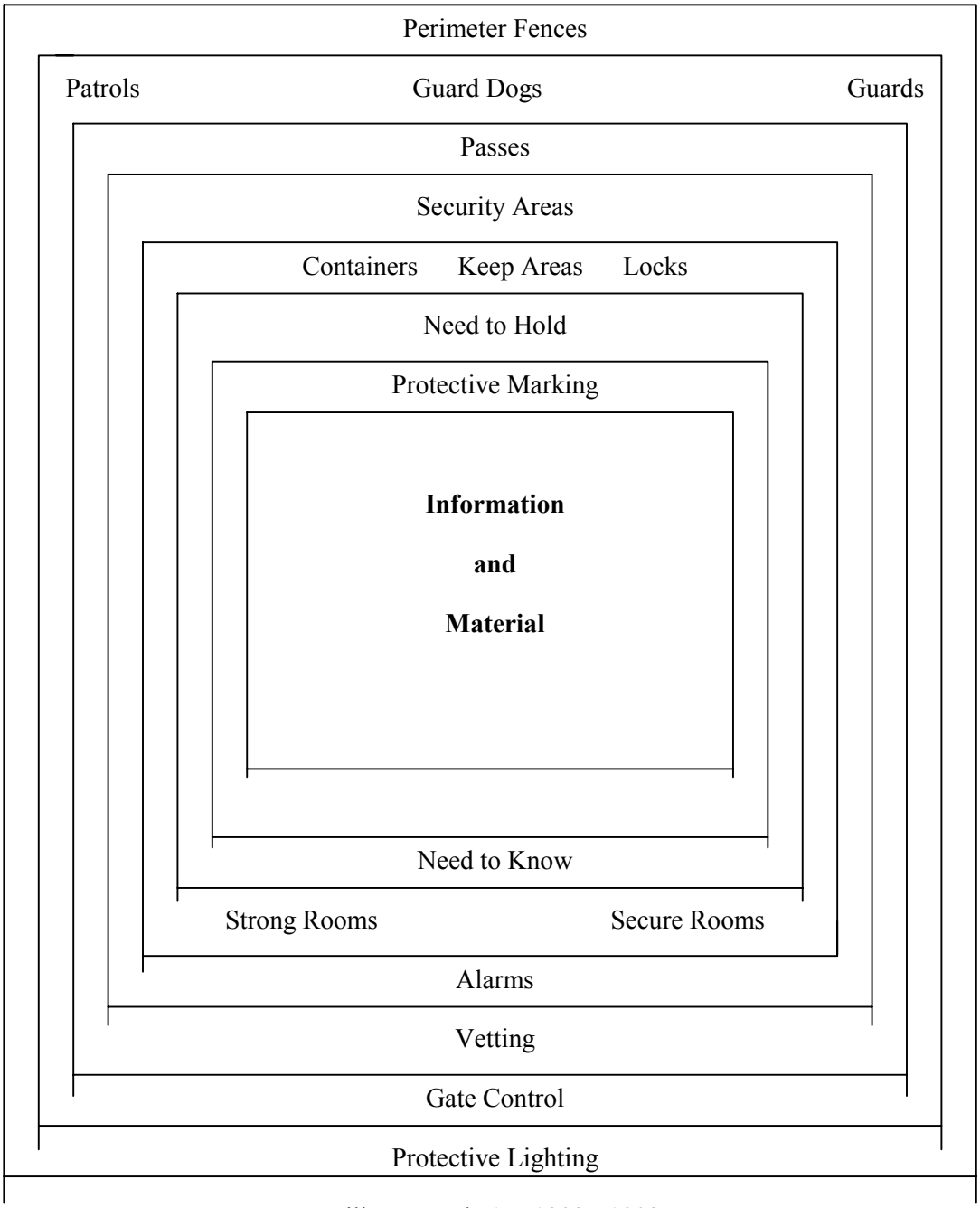
Level	Term	Definition
1	**IMMINENT**	Specific intelligence shows that a target is at a very high level of threat and that an attack is imminent.
2	**HIGH**	Specific intelligence, recent events or a target's particular circumstances indicate that it is likely to be a high priority and the target is at a high level of threat.
3	**SIGNIFICANT**	Recent general intelligence on terrorist activity, the overall security and political climate of the target's general circumstances indicate that it is likely to be a priority target and is at a significant level of threat.
4	**MODERATE**	A target's circumstances indicate that there is potential for it to be singled out for attack and it is at a moderate level of threat.
5	**LOW**	There is nothing to indicate that a target would be singled out for an attack and there is a low level of threat.
6	**NEGLIGIBLE**	A target is unlikely to be attacked. There is a negligible level of threat.

This page intentionally left blank.

ANNEX E TO CHAPTER 1

DEFENCE IN DEPTH

· Official Secrets Acts 1911 - 1989



Military Lands Act 1892 - 1903

This page intentionally left blank.

CHAPTER 2

SECURITY RESPONSIBILITIES

CHAPTER 2

SECURITY RESPONSIBILITIES

General

0201. The Strategic Defence Review (SDR) of 1998 led to significant changes in the way the business of the MOD is conducted. As a result, in September 1999, 2nd PUS commissioned a review to examine the organisation of security in the department. The Security Structures Review (SSR) considered all aspects of security except policing, guarding and vetting. The results of the review were endorsed by the Defence Management Board on 25 January 2001 as DMB(00)12. DCI GEN 148/01 reported the outcome.

0202. This chapter describes the organisation, management and delivery of security in the MOD following the SSR. It sets out the delegations to Top Level Budget (TLB) Holders and Chief Executives of MOD Trading Funds (TFCEs), and the revised responsibilities of organisations and staff involved in determining security policy, those implementing policy, and those providing security support, advice and assistance.

Impact of Security Structures Review

0203. A guiding principle of the SSR was that security is a core business issue and should be firmly embedded in management systems and processes of the Department with ownership of risk unambiguous, and aligned with budgetary authority and accountability. The management of security risk is to complement and mirror the application of corporate governance principles.

0204. Every individual who works for the MOD has a responsibility to promote and maintain security at all times. Directors, heads of divisions, chief executives of defence agencies/GOCOs and commanding officers/heads of establishments are specifically responsible for security within their directorates, headquarters, formations/stations, agencies/GOCOs or units/establishments and are responsible for accepting the risks arising from the risk management process.

0205. TLB Holders remain responsible for implementation of security measures in those Vote funded Defence Agencies for which they, or their senior staff, are Owners. Trading Funds will for security assurance purposes be treated in the same way as TLB Holders, and be held accountable to the Departmental Security Officer (DSO).

0206. Separate guidance is issued on revised responsibilities for dealing with the security of nuclear weapons and nuclear materiel.

Responsibilities of Government Security Departments and Agencies

Cabinet Office

0207. The Prime Minister is ultimately responsible for national security advised by the Cabinet Secretary. The Official Committee on Security (SO) is chaired by the Cabinet Secretary and attended by Permanent Under Secretaries. SO is responsible for formulating policy on all aspects of security co-ordinated across government in consultation with departments carried out through sub-committees and working groups. The Cabinet Office provides the secretariat and draws the threads together, setting government protective security policy and standards which are promulgated in the Manual of Protective Security (MPS), after consultation with departments and after taking advice from the Security Service and the Communications Electronics Security Group (CESG).

Security Service

0208. The Security Service is the UK authority for all aspects of security. It is the principal security adviser to government and is responsible for providing advice to departments and agencies and other organisations on the nature and levels of threats to security from espionage, terrorism and sabotage, and from the activities of those who seek to overthrow or undermine Parliamentary democracy by political, industrial or violent means. In order to counter such threats the Security Service provides advice and assistance on physical, personnel, document, IT and technical security measures and training for departmental staff.

Communications-Electronics Security Group (CESG)

0209. The CESG of the Government Communications Headquarters is the National Authority responsible for all technical issues relating to the security of IT, communications, radar and other such systems, and radiation security. It is responsible for general and specific assessments of the threat of technical attacks on protectively marked information, including that held in IT systems. It is also the National Cryptographic Authority and the authority on the technical threat from SIGINT, hacking and malicious viruses etc. In meeting these responsibilities CESG publishes a wide variety of technical guidance, designs and approves encryption equipment, and produces keying material. CESG helps to formulate policy in this field and contributes to the overall threat assessments produced by the Security Service.

Security Strategy Unit Technical Group (TG)

0210. Technical Group (TG), which operates within the Foreign and Commonwealth Office (FCO), is the National Authority for counter eavesdropping (CE). It is responsible for advising the Security Service on the technical aspects of CE and carrying out related work for the FCO and, in the UK, on behalf of the Security Service.

Security Services Group (SSG)

0211. The SSG provides support to the MOD under a supply and services agreement. The SSG advisory service is free to MOD customers at the point of delivery while other SSG services are charged for on repayment terms. The service may be in response to specific requests from security staff for project management, installation, commissioning and/or maintenance of security equipment and control systems based on set standards. Applications for project support are to be made through PSyAs and Command security staff. They, in turn, may instigate SSG support through D Def Sy for the project. Establishments are not to make direct contact, in the first instance, with SSG.

Responsibilities in the Ministry of Defence

0212. Overall responsibility for security in the MOD rests ultimately with the Defence Council and PUS is a member of the Official Committee on Security (SO). The Director General Security and Safety (DGS&S), is the DSO, responsible for overseeing the implementation and dissemination of protective security policy, the issue of guidance and for incident reporting. The DSO also contributes to the formulation of national security policy and is a member of SO sub committees dealing with information security (SO(IS)), and protective security (ICPS). As part of the process of security assurance required under corporate governance, DGS&S is required to submit an annual report as a Certificate of Assurance to the Defence Audit Committee (DAC).

Role and Responsibilities of the Directorate of Defence Security

0213. A single headquarters policy and standards-setting division, the Directorate of Defence Security (D Def Sy), formed on 1 April 2001 reporting to the DSO. This new division has been created from the former Directorate of Security Policy (DSy(Pol)) and policy elements dealing primarily with industrial security matters and scientific and technical security advice from the former DHQSy division. The Directorate's responsibilities include the newly- created Joint Security Co-ordination Centre (JSyCC) to co-ordinate alerts and warnings of information security incidents, including electronic attacks. The JSyCC will provide a 24-hour/7 day week watch keeping capability. Its role is described at paragraph 0216. D Def Sy is responsible to the DSO for the formulation and promulgation of security policy for the protection of all MOD information, assets and personnel, including international security arrangements for the sharing of MOD information with other governments and with the Defence industry.

0214. D Def Sy has the following principal responsibilities:

a. Contributing to the formulation of government protective security policy and representing the MOD in interdepartmental and international discussions on protective security policy.

b. Formulating and promulgating defence security policy, setting MOD security objectives and providing guidance on their implementation and resource implications.

c. Primary responsibility for nuclear security matters (but on key issues will act only in concert with the Director of Nuclear Policy).

d. Co-ordinating and providing advice to ministers, PUS and CDS on the political and presentational and legal aspects of protective security policy and security intelligence operations.

e. Liaison with the Cabinet Office, Security Service, OGDs and the Civil Police on security policy issues.

f. Developing security policy and providing security advice to companies holding MOD protectively marked assets or information.

g. Advising DCDS(C) on defensive measures to counter the terrorist and extremist threats to MOD personnel and assets in Great Britain and, in consultation with the Counter Extremist Advisory Group (CEAG), setting the counter-extremist alert state for MOD establishments throughout Great Britain.

h. Timely dissemination of security threat information relating to terrorist threats in Great Britain and overseas.

i. Timely dissemination through the JSyCC of electronic threat information relating to the Department's information systems, covering both IT incidents and electronic attack.

j. Oversight of the reporting and investigation of security incidents and leaks of official information by TLB Holders/TFCEs, with particular emphasis on the possible need to revise current security policy, and other remedial action.

k. Serving as departmental focus for the application of UK policy for sensitive document handling and dissemination, and representing MOD on the STRAP management board.

l. Enabling Risk Owners to establish the correct balance of risk to Information Systems by advising on security policy and the residual risk.

m. Advice to MOD and to UK Defence Manufacturers on all technical security matters relating to the overseas release of military information; clearance of UK protectively marked equipment and information at UK and overseas defence exhibitions; and for review of Patent Applications and inventions notified by the general public.

n. Support the DSO in identifying the MOD's security education and training needs and in contributing to the formulation of the policy to meet those needs. (Note: This reflects a responsibility placed on the DSO in the Manual of Protective Security. Exercise of this responsibility will have to take account of the Defence Training Review).

o. Preparation of the annual DSO's report to the DAC, including tasking and collation of TLB Holder/TFCE reports and staffing of follow-up action required.

0215. D Def Sy is accountable through DGS&S to:

a. DCDS(C) and thence to VCDS for the policy on the protection of MOD personnel and assets against terrorists and other extremists including the counter extremist Alert State.

b. The Personnel Director and thence to 2nd PUS for all other aspects of protective security policy.

Role and Responsibilities of the Joint Security Co-ordination Centre (JSyCC)

0216. The JSyCC acts as a focal point for information security intelligence. It maintains a central source of vulnerability and threat information, and promulgates summaries, alerts and rectification directives as necessary. The specific responsibilities of the JSyCC include:

a. Collating progress reports against Threat Change Notices (TCN) and Vulnerability Rectification Directives (VRD).

b. Receiving and collating incident detection information, liaison with the Unified Incident Reporting and Alert Scheme (UNIRAS) and the Federation of Incident Response and Security Teams (FIRST) for all IT related incidents, and determining the nature of response required.

c. Arranging for, and supervising, any necessary external response where inappropriate to be carried out at unit level.

d. Carrying out any necessary post-incident analysis.

e. Supervision of the overall information verification program including provision of generic software toolkits.

f. Maintaining a central register of the Minimum Essential Defence Information Infrastructure (MEDII) element of the Critical National Infrastructure (CNI).

g. Direct control of the verification activities associated with MEDII.

h. Provision of MOD contribution to the National Infrastructure Security Co-ordination Centre's (NISCC) virtual organisation, and related aspects of the CNI protection programme.

i. Provision of awareness and training relating to CIS threats, vulnerabilities, and incident handling.

j. Liaison with similar organisations in UK Government, industry, allies, hardware manufacturers, software providers and the police.

Defence Security Standards Organisation

0217. The Defence Security Standards Organisation (DSSO) was established under the DSO on 1 April 2001 to provide an independent security audit capability and a central source of advice on security implementation issues. The work of the DSSO will in future be integrated into that of the DAC to meet the requirements of corporate governance. The DSSO will include a centralised accreditation function for networked IT systems that cross TLB/TF boundaries. The responsibilities of the DSSO fall into two main areas:

a. **Accreditation.** Provision of a centralised IT security accreditation service, acting as a single source for advice and expertise on MOD's increasingly networked IT systems. DSSO accreditors will advise business managers of the risks to their IT systems and how best to mitigate and reduce them. The decision to accept the residual risk will lie with the business manager in consultation with other stakeholders. If stakeholder interests conflict, resolution will be determined by either DG Info, ACDS (Ops) or CJO in accordance with established crisis response processes.

b. **Security Audit**. Provision of an independent security audit capability to enable the DSO to certify that security policy is being implemented adequately and cost-effectively across the whole of MOD and its Trading Funds. DSSO auditors will focus on assessing the effectiveness of the integrated risk management process of the TLB Holder/TFCE. The precise methodology will be developed in partnership with TLB Holders/TFCEs in a series of pilot audits. Key areas to be addressed include:

(1) Linkage of security risk to corporate objectives.

(2) Common terminology.

(3) Assessment by likelihood and impact.

(4) Dynamic review and reporting.

(5) Effective reaction.

The formal audit process will draw upon the DSO's Annual Report to the DAC to determine the key themes to be examined.

STRAP Administration

0218. There are plans for STRAP administration responsibilities currently carried out by STRAP Security Officers (STRAPSOs) to be re-brigaded under the DSSO. Pending implementation of this change the pre-SSR arrangements are to continue.

Personnel Security Responsibilities

0219. Post SSR, arrangements for the exercise of personnel security responsibilities, including management of risk cases, have still to be finalised. In the meantime the following arrangements will apply:

a. D Def Sy is responsible for Civilians in the Central TLB, DPA and Trading Funds and their non List X contractors, for List X industry (but TLBs are responsible for List X contractors employed at their sites), and for categories such as SCS and MDP managed centrally.

b. The single Services are responsible for their Service personnel wherever they are employed, for Civilians employed in Service TLBs (except for categories managed centrally), and for contractors employed at their Service sites.

c. The DLO and PJHQ are responsible for Civilians employed in their TLBs (except for categories managed centrally), and for contractors employed at DLO and PJHQ sites.

Responsibilities of TLB Holders/Trading Fund Chief Executives

0220. Responsibility for the implementation and risk management of security policy and standards has now been formally delegated to TLB Holders by means of a single letter of delegation from PUS. Each TLB Holder is required to nominate a Security Risk Manager to advise the TLB on the balance between business needs and security requirements, taking account of affordability, and act as a TLB point of contact with

the DSO. They will form the membership of a new DSO advisory group, the DSO's Risk Managers Forum (DRMF). TLB Holders and TFCEs will be responsible for maintaining an audit trail of their risk management decisions, and for making a formal annual report to the DSO on the state of security in their TLB/TF. An extract from PUS's letter of delegation to TLB Holders is shown below:

I look to you to ensure that Departmental security policy and standards set out in JSP 440 are implemented across your TLB. Your Principal Security Adviser (to be appointed by you) will support you and should be consulted whenever you are unclear about specific delegations or need more general advice. Should you or your Principal Security Adviser be unsure about the interpretation and exercise of the delegations or need specialist advice, you should consult the Departmental Security Officer.

Specific Authority

Authority for the implementation of Departmental security policy and standards (set out in JSP440 and other policy guidance) in your TLB.

Authority to take necessary timely action on receipt of terrorist and other security threat alerts, and when necessary, the co-ordination of BIKINI Alert State and other counter-measures for all units/establishments in your TLB area.

Authority to exempt units/establishments in your TLB area from compliance with armed guarding and other prescribed security measures, within the limits for variation set out in JSP 440 and other MOD policy guidance.

Authority for accrediting IT systems that are delegated to you by the Departmental Security Officer (DSO).

Authority to undertake a programme of assurance activities to verify internal security control processes. This will be subject to audit by the Defence Security Standards Organisation (DSSO).

Responsibilities

You should ensure that your decisions on security adhere to Departmental risk management guidelines.

You should, in consultation with the DSO, appoint a Principal Security Adviser (PSyA) who will be your source of authoritative day-to-day advice. The PSyA should meet minimum core competencies and have received the appropriate training. The PSyA may be appointed from your TLB, or be provided from another, under agreed arrangements. He or she should consult the DSO for specialist advice when needed, including on any cross-TLB issues.

You should nominate a 'risk manager' to advise you on the balance between your business needs and the security requirements, taking account of affordability, and to act as the point of contact for the TLB with the DSO.

You should invest in the necessary training and education to ensure that all staff in your TLB are adequately trained and have the right level of security awareness.

You must agree an audit programme for your TLB with the DSO.

You must submit an annual report to the DSO on the state of security in your TLB.

Responsibilities of Principal Security Advisers

0221. The former Sector Security Authorities were abolished on 1 April 2001. In their place, TLB Holders and TFCEs are to appoint their own Principal Security Adviser (PSyA). The services of another TLB may be chosen to provide the relevant security advice but the responsibility and accountability for the application and maintenance of security in their area is vested in the TLB Holder/TFCE. The role of PSyAs is to provide corporate security advice to the Management Board of the TLB Holder/TFCE and oversight and direction of security across the TLB/TF. The following are specific PSyA responsibilities:

a. Advice to the TLB Holder/TFCE and the Management Board on all security issues that have a corporate bearing on TLB/TF business. This includes advice on:

(1) Interpretation of Departmental security policy.

(2) Evaluation of the security risk applicable to the TLB/TF.

(3) Implementation measures.

b. Strategic oversight of security activity across the TLB/TF, ensuring compliance with policy as implemented within the context of risk-based security management.

c. Representing the TLB/TF corporate interests in all security activity within the department, consulting with business units and agencies as appropriate.

d. Providing the TLB/TF focal point for the DSO and D Def Sy.

e. Liaison with other PSyAs and co-ordinating the sharing of security support activities.

f. Liaison with the police and other security agencies in government and industry as necessary.

g. Ensuring procedures for reporting and investigating security incidents are followed, where necessary conducting investigations.

h. Ensuring security surveys and periodic inspections are carried out in all subordinated establishments.

i. Undertaking a range of tasks associated with those IT systems that are specific to the TLB/TF, including accreditation, of those IT systems for

which the TLB/TF has been delegated responsibility, ensuring compliance with security requirements, and reporting IT security incidents.

j. Development and implementation of revised structures as necessary to meet the full range of TLB Holder's/TFCE's responsibilities that flow from the Security Structures Review.

k. Provision of security guidance to subordinate headquarters, units and establishments across the TLB/TF as necessary.

l. Development of a security culture within the TLB/TF that is cost-efficient and makes use of best practice within the context of risk management as applied to business needs.

Categorization of Establishments

0222. In order to determine priorities for the allotment of security effort, each establishment should be allocated a security category. Categorisation of MOD establishments will maintain a consistent baseline across the Defence spectrum and assist with the risk management process that will inform resource allocation decisions. It is, therefore, important that TLB Holders/TFCEs are able to give their establishments a security profile, assessed against common definitions. Details on the categorization of establishments are at Annex A.

0223. The categories into which establishments are placed must be reviewed at regular intervals and on the following occasions:

a. On formation, reorganisation or amalgamation of an establishment.

b. When significant changes occur in the role or organisation of an establishment or in the type of equipment held.

c. When there is a major change in accommodation and guarding arrangements.

Security Surveys, Inspections and Audits

0224. The following definitions apply:

a. **Survey**. A detailed, pre-planned security examination carried out by a specialist team to examine, report and make recommendations on the protective security requirements of an establishment.

b. **Inspection.** A periodic, on-site review of compliance with security orders, regulations and instructions, conducted by a security team tasked by the TLB Holder/TFCE that owns the risk at the establishment concerned.

c. **Audit.** An independent review by the DSSO of the systems and structures in place to support the TLB Holders'/TFCEs' security risk management processes.

0225. TLBs/TFs are required to carry out a security survey when an establishment is first formed, is reorganised and changes its role, or on completion of major works services. The comprehensive survey report will be the baseline against which future protective security of the establishment will be measured. Additional security surveys may be conducted in response to special requirements as required by TLBs/TFs.

0226. A new regime has been introduced to reflect the delegated responsibilities for security risk management and a more flexible approach managing all aspects of the changing threat. Threats to Defence establishments vary widely, as do their vulnerabilities. Although every establishment should be subject to periodic formal security inspection, the programme should reflect these differences. In determining the frequency of inspections for establishments within their area, TLBs/TFs will need to consider various factors. These will include: the criticality of the establishment's output in meeting MP objectives, the risk profile, the outcome of previous inspections and audits, turnover of key personnel and any mandated requirements. Security inspection reports will provide a major input into the DSO annual report to the DAC. TLB Holders/TFCEs may elect to supplement formal inspections by advisory visits and by the completion of security questionnaires. Further detail on inspections and guidelines for periodicity are at Annex A.

Special Security Surveys

0227. In addition to the initial security surveys referred to above, certain establishments will require surveys of a specialist nature, for example counter sabotage surveys, air transport security surveys, aircraft physical security surveys and counter terrorist surveys. PSyAs and Command security staff are to arrange the frequency and implementation of these surveys to meet their needs.

Responsibilities of Command and other Security Staffs

0228. Command security staff officers and other staff officers whose responsibilities include security are responsible for:

a. Advice to their Commanders/Directors on all security matters.

b. The processing of security intelligence and the production of up-to-date assessments of the threat to security. This includes the dissemination of threat assessments.

c. The preparation and issue of security standing orders and instructions.

d. The provision of assistance and advice, and the issue of instructions, to subordinate staffs and establishments on all aspects of security. This includes the planning, co-ordination and application of protective security measures throughout the formation including those for exercises and operations.

e. Advising on the granting to establishments of waivers and exemptions from the baseline measures and mandatory standards of JSP 440 having first obtained authority from D Def Sy when this is necessary.

f. Contributing to the Operational Security (OPSEC) staffing process for exercises and operations with particular reference to the formulation of the threat and recommendations for protective security measures.

g. Tasking, and direction where appropriate, of security units.

h. Ensuring the maintenance of a close liaison with the Civil Police and the co-ordination of security contingency plans when necessary.

i. Action to ensure security incidents are investigated and that the procedures laid down for reporting and investigating breaches of security are followed. Security staff is responsible for ensuring that counter-compromise action is taken and for making recommendations on the security aspects of breaches to the Commander. Records and statistics concerning breaches should be kept to enable the state of security in the formation to be assessed and the adequacy of the existing security measures to be reviewed.

j. Actioning Parliamentary Questions and Parliamentary Enquiries on matters relating to the implementation of security as directed by Min AF and copying the reply to Min AF and D Def Sy.

k. Advice to the Commander, staff and establishments on security education and training, including its organisation and conduct.

l. The provision of security support to sponsored organisations.

m. Advice to the relevant staff on:

(1) The security aspects of new projects and maintenance works services in the early planning stages.

(2) Priorities for the issue and replacement of security furniture and equipment.

(3) Requirements for works services arising from the recommendations of protective security survey and inspection reports.

n. Regular review of the Developed Vetting Master List (DVML) of posts, where held.

o. Contributing to the TLB/TF annual report to D Def Sy.

p. Ensuring that security surveys and periodic inspections are carried out on all subordinate establishments.

q. Ensuring close liaison is maintained at all levels with appropriate security units.

Responsibilities of the Head of Establishment (HOE)

0229. HOE are responsible for all aspects of the security of the establishments under their command and control and for personally accepting the risks arising from the risk management process.

0230. The responsibilities of the HOE include bringing to the attention of all personnel specific aspects of protective security as detailed below:

a. **General.** Personnel are to be reminded of:

(1) Their responsibilities under the Official Secrets Acts.

(2) The threat and their responsibilities in countering it.

(3) The provisions of security standing orders. (Subjects that should be considered for inclusion in security standing orders are listed at Annex B).

(4) The need for vigilance at all times.

(5) The need to report all suspicious occurrences and anything which may lead to a breach of security without delay.

(6) The requirement to report all contacts with persons from countries to which special security regulations apply, and contacts with persons from other foreign countries which give rise to suspicion.

(7) The need to report, well beforehand, proposed visits to or from countries to which special security regulations apply or travel in their controlled air, rail or shipping lines.

(8) The requirement to ensure security approval exists for official visitors attending briefings, discussions or making use of establishment or site facilities and also contractors.

b. **On appointment to a post giving access to protected information.** The aim is to ensure that all individuals whose duties include handling protected information:

(1) Understand their security responsibilities.

(2) Know the establishment system of custody and handling of protected information, documents and material necessary to carry out their duties.

(3) Understand the principles of 'need to know' and 'need to hold'.

(4) Are aware of the action to be taken on the loss or compromise of protected documents or equipment.

(5) When a proposal to job share a security post is received the HOE should weigh the consequences of such sharing against the possibility of a loss of accountability or any weakening of responsibility for the control of either Physical, Documentary, IT or Personnel security. In the first instance the HOE should contact his own PSyA or Command security staff for advice.

c. **On specific occasions.** The aim is to ensure that all Service and civilian staff are made aware of their responsibilities for security on the following occasions:

(1) Before taking part in operations.

(2) Before taking part in exercises.

(3) Prior to travel, either on duty or leave, to or through countries to which special security regulations apply. This includes members of the reserve and officers of the cadet forces.

(4) When on duty at open days, exhibitions, demonstrations, or trials of protected equipment in any official capacity, for example as guards, drivers, or exhibitors.

(5) When attending courses which include foreign students.

(6) At conferences, seminars and meetings to which foreign representatives are invited.

Responsibilities of the Establishment Security Officer

0231. The HOE is to appoint an establishment security officer (ESyO) who is directly responsible to his HOE for the implementation of security policy. It is mandatory that the ESyO is correctly trained in his responsibilities and, unless already trained as a security officer, attends a security officers' course either prior to, or immediately after, assuming his appointment.

0232. The responsibilities of the ESyO include:

a. **Threat assessment and planning.** Assessment of the threat to the security of the unit and the planning and implementation of counter measures.

b. **Security standing orders (SSOs).** The production and promulgation of SSOs. A guide to the headings is at Annex B.

c. **Security education and training.** The education of all personnel on the threat and their responsibilities for countering it and the training of individuals having specific security duties and responsibilities.

d. **Vetting register.** The supervision of the establishment vetting register where applicable. The register is to include a list of posts in the establishment that require SC or DV security clearance, the name of the post holder, his/her clearance level, the expiry date and any limitation to the clearance.

e. **Security orders, regulations and instructions.** Acquainting themselves with relevant current security policy, orders, regulations and instructions and advising the HOE on their implementation. References for security officers are listed at Annex C.

f. **Protective security.** The maintenance of protective security through systematic reviews, checks and inspections to ensure that:

(1) The recommendations of security surveys and inspections have been implemented or that the security staff have been informed of the reason for non-compliance.

(2) SSOs are comprehensive, understood and observed.

(3) Security equipment such as PIDS, IDS and access control systems are functioning correctly.

g. **Initial investigations.** Carrying out initial investigations into breaches of security.

h. **Reporting.** Keeping the HOE informed on all matters affecting the security of the establishment.

i. **Security liaison.** Liaison with the security staff, the local security unit and the local Civil Police.

j. **IT security.** Where so appointed, ensuring the measures for IT security promulgated in Volume 3 of JSP 440 are fully instigated.

k. **Supervision.** Ensuring that the holders of any subordinate security appointments are adequately briefed for their duties.

Lodger Units

0233. Lodger Units will normally conform, in the first instance, to their own Security Regulations, but they are also responsible to those of the host establishment, whose HOE has a duty of care to ensure that security within the establishment does not fall below the standards set out in JSP 440 and his own single service or HQ Security Instructions. Where conformity is not possible deviations are to be noted in a written agreement between the host establishment and the lodger unit, endorsed by the PSyA of the host establishment TLB/TF and the chain of command of the lodger unit. In principle, security responsibilities must lie where they can best be exercised. If however the lodger unit has its own secure perimeter a different security regime may apply within that perimeter, if this is considered to be in the best interest of security. In the normal course, lodger units will, whenever possible, be subjected to security inspections and audits at the same time as the host establishment and these may, if appropriate, be conducted by the host unit security authority, even if the lodger unit is required to submit its own annual report or be subject to inspection.

Copies of all inspection/audit reports will be forwarded to the chain of command of the lodger unit.

Responsibilities of Security Units

0234. Security units (see Glossary) operate under the direction, as appropriate, of PSyAs and Command security staff. Security units undertake the following tasks:

a. The provision of advice to the security staff and establishments, where appropriate, on factors affecting the threat assessment and on protective security measures.

b. The acquisition of security intelligence.

c. The collation of all security information to support and assist security intelligence operations.

d. The provision of security advice and assistance to establishments.

e. The investigation of security incidents, which may include:

(1) Activities of foreign intelligence services involving espionage, sabotage, subversion, or terrorism. Such investigations are carried out in conjunction with the appropriate civilian agencies.

(2) The loss or compromise of protectively marked material, in particular, documents and leaks of official information.

(3) The loss or compromise of protectively marked or protected material, including records of combination lock settings and security keys.

(4) The loss of arms, ammunition or explosives.

(5) Certain aspects of criminal activity affecting security. Such investigations are conducted jointly, where appropriate, with the Service Police or MDP, in conjunction with the appropriate civilian authorities.

f. Protective security surveys, and security inspections of establishments as directed by PSyA and Command security staff.

g. The formulation of protective security plans for particularly sensitive establishments.

h. The maintenance of records and statistics.

i. The provision of technical advice on security planning and where appropriate specialist resources for public occasions such as open days or Royal/VVIP visits.

j. The provision of technical advice to the security staff in planning the protection of personnel.

k. The vetting of locally engaged civilians overseas for access to official information.

l. Where appropriate, the screening of persons for access to military areas and establishments.

m. The provision of assistance to commanders, staffs and establishments in security education and training.

n. Liaison with other Service agencies.

o. Liaison with allied and civilian security agencies.

Other Security Appointments

0235. According to the role, size, sensitivity and dispersion of an establishment, or grouping of establishments, other security appointments may be necessary. Where other appointments are made, co-ordination of security effort within an establishment remains the responsibility of the ESyO. Examples of other security appointments include:

a. **Branch Security Officer (BSO)/Unit Security Officer (USO).** Where it is justified by size, dispersion or the existence of a specialized installation, BSOs/USOs should be appointed. In the case of a specialized installation, an officer with a knowledge of the specialist equipment should be nominated.

b. **Control Officer.** Establishments which hold documents protectively marked TOP SECRET, and documents which require special handling such as those marked ATOMIC or ATOMAL, are to appoint a control officer who is to be personally responsible for the safe custody of and accounting for all such documents. Details are given in Chapter 4.

c. **IT Security Officer (ITSO).** Establishments are responsible for appointing IT security officers as required by JSP 440 Volume 3.

d. **Project Security Officer.** Personnel appointed to plan and oversee the implementation of the security measures required in the realization of major projects involving protectively marked information.

e. **Station Security Officer/Garrison Security Officer.** Personnel appointed to co-ordinate the implementation of security measures across a number of establishments in a station or garrison area.

Reporting of Incidents

0236. It is important that all Defence related suspected, attempted, or actual security incidents and weaknesses are reported to the appropriate PSyA and Command security staff. PSyAs and Command security staffs are to stipulate their requirements for upward reporting of incidents (losses, compromises, breaches, weaknesses and attacks) on their establishments. The following incidents are always to be reported to D Def Sy via the chain of command:

a. Any terrorist act or incident likely to have had terrorist involvement (e.g. suspected recce of an MOD establishment).

b. Incursions into MOD sites which involve a significant threat to the security of that unit or establishment.

c. Significant losses or theft of arms or explosives and/or significant quantities of ammunition.

d. All cases of suspected sabotage and other cases of malicious damage to assets where the damage would equate to that requiring the protective marking CONFIDENTIAL or above.

e. Any loss or theft of documents or material, where espionage is thought to have been involved or where there is likely to be media, public or parliamentary interest, or embarrassment caused.

f. Leaks of official information to the media.

g. All instances of hacking into MOD CIS systems, and of significant damage due to destruction or corruption of information on MOD CIS systems, as a result of computer viruses to be reported to the JSyCC (see also JSP 440 Volume 3 Chapter 10).

h. All personnel security cases involving appeals against denial or withdrawal of security clearances and any other personnel security cases likely to attract parliamentary and/or media attention or otherwise cause embarrassment to the MOD. Where appropriate, incidents should also be

reported to security units and the Service Police, MDP or Civil Police in accordance with single-Service instructions.

Security Incidents - Mandatory Reporting to Ministers

0237. Guidelines on the reporting of security incidents that might attract public, Parliamentary or media attention and require involvement of Ministers are at Annex D. The instruction identifies which types of incident are to be reported to Ministers in an accurate and timely way, the methods to be used and contact telephone numbers. Particular attention is drawn to the requirement to include D Def Sy as an information addressee at all stages of the reporting process. The initial report signal format is at Annex E. D Def Sy is required to maintain data on all security incidents reported in order to provide a record of remedial action, particularly in relation to any need to amend security policy.

0238. Losses. For the purposes of reporting and investigation, losses are categorized as follows:

a. **Category 1.** All TOP SECRET, COSMIC/ATOMAL ATOMIC and comparted information including Codeword material. Also COMSEC material (which means all documents, aids, devices or equipment, including CRYPTO material, associated with the securing or authentication of telecommunications).

b. **Category 2.** SECRET (including NATO and other IDO) material.

c. **Category 3.** CONFIDENTIAL (including NATO and other IDO) material.

0239. Aggregation. It is recognised that the aggregation of multiple losses of information at the Category 2 level could warrant that information being raised to the Category 1 level overall. PSyA and Command security staff should try and ascertain whether or not the losses in question fall into this category and, if they consider this to be the case, to inform D Def Sy.

0240. STRAP. The loss and/or compromise of STRAP material should be reported and investigated in accordance with the security regulations laid down in the STRAP Manual (JSP 440 Volume 5).

0241. Reporting. During working hours, incidents should normally be reported to the PSyA and Command security staff. For significant issues that occur outside core working hours, the MOD maintains an Information Security Duty Officer (ISyDO), which is a role fulfilled by members of D Def Sy or JSyCC staff. Some TLBs/TFs maintain a 24 hour Duty Officer who will be responsible for upward reporting to the

JSyCC/ISyDO. Further details on incident reporting are contained in Chapter 11 of Volume 3.

Security Investigations

0242. PSyA and Command security staff are responsible for the overall co-ordination of security investigations within their areas following submission of an immediate report, either by signal or e-mail, within 24 hours of the loss or compromise of the protectively marked material being confirmed or suspected (see Annex F) by the establishment concerned. Early initial reports to PSyA and Command security staffs allow a rapid judgement to be made as to the severity of the incident and minimise any delay likely to accrue in returning to normal working whilst any required security response takes place. It will also provide an opportunity to provide specialist advice and guidance to the establishment at which the incident occurred. After the immediate report has been sent, the following procedure should be followed:

a. **Initial report.** An initial report should be submitted, in writing (either as a letter, signal or e-mail) to the appropriate PSyA and Command security staff, within 48 hours of the immediate report.

b. **Progress reports.** Progress reports should be submitted, in writing to PSyA and Command security staff, within seven days of the immediate report, giving an update on the progress of the investigation. If the investigation is not complete when the first progress report is due, PSyA and Command security staff should be consulted on the frequency of future progress reports.

c. **Final report.** The final report should be forwarded, in writing to PSyA and Command security staff, once the investigation is completed. It should be comprehensive and include recommendations for action to be taken.

Notes:

1. Where a major security investigation is required, at least one member of any investigation team used must be aware of the requirements of the Police and Criminal Evidence Act (PACE).

2. In the case of the MDP, Service Police, members of the Intelligence Corps, RN Area Security Teams or regional RAF Provost and Security Services (P&SS), such knowledge can be assumed. In all other cases, staff acting as security investigators must be formally registered with JSyCC on behalf of the Departmental Security Officer (DSO).

3. Minor breaches' investigations can be performed on behalf of the Head of Establishment by local security staffs.

4. All serious breaches are to be reported to D Def Sy.

0243. Care must be taken to assign an appropriate protective marking to all reports, and to use appropriate communications channels.

Disciplinary and Criminal Considerations

0244 In addition some incidents may also involve disciplinary and criminal considerations.

0245. Malicious damage and theft. Deliberate damage to, and theft of, MOD assets are clear indications of a criminal act having occurred, **and other than in cases where a serious breach of National Security has also occurred**, the pursuit of such incidents will normally be through the MDP or Service Police as appropriate.

0246. Immediate incident report. Unless the criminal activity is detected whilst in progress, when MDP or Service Police as applicable should be contacted directly, in all other cases an Immediate Incident Report should be raised to the PSyA or Command security staff who will ensure that the appropriate Police authority is contacted.

0247. Physical infiltration. The physical infiltration of a MOD site by unauthorised persons should be dealt with by either local security staffs, through the MDP or Service Police as appropriate, as laid down in this volume and reported. Any collateral incidents (e.g. theft) should, however, be assessed against the guidance in this Chapter.

Post Incident Analysis

0248. PSyAs and Command security staff are responsible for ensuring that copies of all final reports, about lost or compromised material, are sent to their originators or owners at the close of the investigation. They are also responsible for ensuring that any counter-compromise action is completed as necessary. The HOE is responsible for ensuring that an Aftercare Incident Report (AIR) is raised to the DVA for all instances where MOD or contractor personnel have been involved in either misuse of MOD resources and/or criminal activity.

Action on Loss or Compromise and Levels of Authorization to Write Off

Action to be Taken in the Event of Loss or Compromise

0249. When protectively marked material is presumed lost or believed compromised, it is important that the circumstances should be reported to the appropriate PSyA and Command security staff.

Loss in Transit

0250. When material has been lost in transit between establishments, it is the responsibility of the dispatching establishment to take all the necessary action and, where appropriate, to inform the originator or owner of the material.

Loss outside MOD Establishments

0251. Whenever protectively marked material is lost outside MOD establishments, the following urgent action is to be taken by the loser:

a. Take all reasonable steps to effect recovery, e.g. by reporting the loss to the local security unit, the Civil Police, transport authority and lost property office as appropriate.

b. Notify, by the quickest means, the ESyO of the dispatching, originating or parent establishment who will then follow the reporting procedure.

Loss in Emergency Conditions

0252. When protectively marked material is lost under emergency conditions e.g. fire, flood, aircraft crash, disaster at sea, armed attack etc every reasonable effort is to be made to recover or account for any residue or debris.

Authorization Levels to Write Off Losses

0253. **A**uthority to write off lost material is as follows:

a. **Category 1.**

(1) All TOP SECRET – PSyA and Command security staff (at one star level).

(2) All ATOMIC and Codeword - to be referred to the appropriate agency for approval.

(3) COMSEC - An action copy of all CRYPTO losses should also be sent to the appropriate MOD HQ and Single Service Communications Authorities.

b. **Category 2.** Designated PSyA and Command security staff officers.

c. **Category 3.** HOEs/COs/Directors.

d. NATO and other IDO material of all categories are to be referred to the NATO Office of Security (NOS) for NATO material or the appropriate Security Office of the IDO concerned and copied to MOD DIS Sy (IDR).

Note: Authority to write off losses, as stated above, is only given from a security standpoint. It in no way gives authorization to write off the sums of money that may be associated with losses. This is covered in JSP 414.

0254. Should PSyA and Command security staff consider any loss or compromise of such significance as to warrant attention by Ministers then D Def Sy should be informed immediately.

Leaks of Official Information

0255. Leaks usually take the form of reports in the public media which appear to involve the unauthorised disclosure of official information (whether protectively marked or not) that causes political harm or embarrassment to either the UK Government or the Department concerned. Such disclosure may have been made either orally, whether deliberately or carelessly, or following the unauthorised sight or passage of a document. Information that is formally reported as lost to a security authority, and subsequently appears in the public media, should not be treated as a leak but judged to be a compromise of lost information and treated as a loss.

0256. First news of a leak may come direct from a journalist attempting either to verify the information obtained or wishing the Department or agency to know what access to official information has been gained. In the rare cases where this occurs prior to publication, it may be possible to seek an injunction to prevent publication.

0257. Leaks of official information are to be reported to the appropriate PSyA or Command security staff in the first instance. Where the leak is judged to be serious, the PSyA or Command security staff are to bring it to the attention of D Def Sy as soon as practicable, and within 24 hours if possible. The consequences of leaks of official information are considered serious when they undermine government policy or cause embarrassment to the government. Examples are:

a. The premature leaking of information on Defence Estimates or other financial details.

b. The leaking of MOD correspondence on issues that are controversial at the time.

c. The leaking of details of overseas defence equipment negotiations prior to formal agreements being signed.

0258. The following factors need to be taken into account by the relevant PSyA or Command security staff in preparing to report the incident as a leak to D Def Sy:

a. The medium/media and journalists (if known) concerned.

b. The intrinsic importance of information leaked. (If there is any doubt as to whether or not the information is important, D Def Sy should be consulted for advice).

c. How widely the information was circulated and in what form.

d. Can a specific document be identified for the contents of the leak.

e. The identity, if immediately apparent, of the source of the leak.

f. Whether or not the Official Secrets Acts are believed to have been breached, if immediately apparent.

0259. In general there is likely to be advantage in pursuing a leak investigation in those cases where:

a. A specific document can be identified from the contents of the leak;

b. The authorised circulation of the leaked document was small; or

c. It has been possible to take the decision to investigate promptly.

0260. D Def Sy, in conjunction with the relevant TLB/TF, will seek advice from the DSO as to whether the details of the case warrant an investigation by the PSyA, Security Unit, Service Police or MDP. This option must be considered before such an investigation is initiated since an investigation that may result in criminal proceedings must be conducted in accordance with the Police Codes of Practice. D Def Sy will take all necessary upward reporting action within the Department where a serious leak has been identified or is strongly suspected.

Waivers and Exemptions

0261. The procedures relating to waivers and exemptions for IT and nuclear assets are described respectively in JSP 440 Volume 3 Chapter 1 and Volume 4 Chapter 1. For all other waivers and exemptions to JSP 440 Volume 1 the rules are detailed below.

0262. The Baseline Measures for protecting the confidentiality of protectively marked information and material, and the physical security standards for the protection of arms, ammunition and explosives are mandatory. No material in this category is to be held if the mandatory standards are not met, unless a deviation in the form of a waiver or exemption has been issued by the appropriate authority. Waivers and exemptions can be granted by TLB Holders/TFCEs and CinCs on their own authority. Exemptions need to be referred to D Def Sy if they involve the assets of other government departments being placed at risk and therefore require Cabinet Office agreement. A list of waivers and exemptions is to be included in the TLB Holder/TFCE annual report to D Def Sy.

0263. Definitions of waivers and exemptions (other than for nuclear and IT assets) are:

a. **Waiver.** A waiver is a risk management tool that allows rules to be waived, in extraordinary circumstances, for periods of up to one year, when it is judged that a temporary deviation will not result in any vulnerability being exploited. Accordingly, a waiver gives approval for the temporary deviation from the mandatory standards in circumstances where:

(1) Essentially the same level of security is afforded and compensatory measures are not required; or,

(2) A vulnerability has been created and acceptable compensatory measures have been applied; or,

(3) A vulnerability exists and, despite the application of all feasible counter measures, remains extant.

b. **Renewal.** If renewal of a waiver is approved, details are to be notified by the PSyA or Command security staff to D Def Sy.

c. **Exemption.** An exemption is similar to a waiver but applies where there is a need for long-term dispensation. The likelihood of a vulnerability being exploited will increase with duration, frequency and predictability. Accordingly, an exemption will only give approval for the long-term deviation from the mandatory standards in circumstances where:

(1) Essentially the same level of security is afforded and compensatory measures are not required; or,

(2) All feasible compensatory measures have been taken and nothing more can be done.

d. **Review.** Exemptions are to be reviewed every 5 years.

Other Security Related Responsibilities

0264. It is necessary security staffs to be aware of the general state of security and the effectiveness of protective measures in their areas of responsibility. Within the chain of command this is achieved by such means as the receipt of security survey/inspection reports, the reporting of breaches of security and a close working relationship between the security staff, security units and ESyOs. It is equally important for the DSO to be able to monitor the overall state of security and the effectiveness of protective measures within the MOD as a whole.

Relations with the Intelligence Staff

0265. Where appropriate, but particularly in Service HQs, the security staff should maintain close liaison with the intelligence staff. In overseas commands both security and operational intelligence assessments should normally be combined to give commanders a complete and balanced intelligence picture.

Liaison

0266. In addition to normal staff liaison and inter-Service consultation (through local security and intelligence committees, where they exist), contacts are to be maintained at staff level with other national and international HQs and with appropriate local security organisations and civil authorities. In parallel with this, security staffs are to ensure that contacts between security units and the Civil Police are established and maintained. Contact with the Security Service and Metropolitan Police Special Branch (MPSB) is only to be carried out through D Def Sy unless authority has been previously been granted for direct contact.

Financial Economy

0267. Recommendations for works services frequently involve high costs in materials and labour charges but, while the need for economy is recognized, this must not inhibit security units from making recommendations necessary to achieve proper security protection. It is the task of PSyA and Command security staffs to examine recommendations for security works services ensuring that only those that are justified on security grounds are given their support. Where high costs are involved, security staffs may require security units to suggest alternatives, with their advantages and disadvantages, to help determine the most cost-effective measures.

Protection against the Threat

0268. It is the responsibility of PSyAs and Command security staff to make an assessment of the local threat from espionage, sabotage, subversion and terrorism to establishments in their areas of responsibility. They should give advice on the protection of establishments to include further precautions to be taken if the threat increases. Responsibility for ordering protective measures against terrorist attack is usually vested in the operations/security staff. The security staff is responsible for

providing assessments of the threat from terrorism, and for the planning and co-ordination of protective security measures to counter the threat. In Great Britain assessments are disseminated by D Def Sy. Overseas and in Northern Ireland, assessments are made and disseminated by commands except that in the case of HM ships visiting foreign ports the threat assessment at the time of the visit will be promulgated by signal by DI RA (Coord). (Chapter 7 gives details of counter terrorist measures).

Key Points (KPs)

0269. The Director of Military Operations, through MO2, is responsible for the direction and staffing of KP policy. Single-Services are responsible for nominating their own KPs and passing details to the Joint Planning Staff (JPS (UK)). JPS (UK) collates these and forwards them, through the MOD KP Committee, to the Cabinet Office KP Committee for endorsement. Once endorsed, KPs are included in JPS (UK) KP Lists. Advice on the security measures at KPs is the responsibility of MOD, PSyAs and Command security staff. Specialist security units are responsible for conducting KP surveys. Responsibility for deciding on the criteria for selection of KPs abroad rests with CINCs, advice on their protection being given by the Command security staff and the local security unit (see Glossary). There will be a need for co-ordination of KPs protection plans in overseas theatres to take account of the requirements of all Service and civilian KPs. The principles governing sabotage planning and the protection of KPs are currently under review.

Amendments to JSP 440 Defence Manual of Security

0270. If PSyAs, Command security staff, HOEs, ESyOs or security units feel that the policy or any of the instructions or guidance contained within this manual are inappropriate or incomplete and require deletion or amendment they are to inform D Def Sy, through their chain of command. D Def Sy will consider the matter and if appropriate, review the policy and take any necessary amendment action.

ANNEX A TO CHAPTER 2

CATEGORISATION OF ESTABLISHMENTS AND SECURITY INSPECTIONS

Introduction

1. The adoption of a combined matrix for categorization of establishments takes account of the full threat spectrum and Risk Impact Level. It facilitates a comprehensive approach to security inspections to include, where relevant, personnel, physical and procedural security measures within the GSE/LSE Inspection (GLI) of CIS installations within sites contained in Chapter 12 to JSP 440 Volume 3 Issue 2. This combined matrix is shown in outline below:

Asset Category	Risk Impact Level	Guarding Category		
		P1	P2	P3
A1	High			
A2	Medium High			
B1	Medium			
B2	Medium Low			
C1	Low			
C2	Very Low			

2. Categories A1-C2 relate to all aspects of the threat to the security of information and materiel (assets) and are based on the new definitions below. The combined matrix to be used in determining the risk profile of an establishment is produced by bringing together separate assessments on all aspects of the threats to information and material (assets), and on the threat to life posed by terrorism. The former involves selection of a category in the range A1-C2; the latter a category in the range P1-P3. In each case, the categories selected are consistent with the Level 2 matrix of Risk Impact Levels referred to in the Risk Management Guidance at Annex C to DSO Guidance Note No 2.

Categorization Definitions

3. The definitions to be used in determining the categorisation of an establishment in relation to the threats to information and material (assets) are as follows:

Category A1. (Risk Impact High). Establishments with a nuclear role and holding nuclear weapons or Special Nuclear Material (SNM).

For example:

See JSP 440 Volume 4.

Category A2. (Risk Impact Medium High). Establishments holding assets or carrying out an exceptionally sensitive or critical role, the loss, disruption or compromise of which would cause *exceptionally grave damage* to the operational effectiveness or key business output of the TLB/TF or MOD.

For example:

Establishments, including branches of HQs, with an exceptionally sensitive or critical role; or whose main outputs depend upon processing information on a CL1 CIS system; or carrying out TOP SECRET research and development activity of major importance to UK defence capability.

Category B1. (Risk Impact Medium). Establishments holding assets or carrying out a very sensitive or critical role the loss, disruption or compromise of which would cause *serious damage* to the operational effectiveness or key business output of the TLB/TF or MOD.

For example:

Establishments, including branches of HQs, with a very sensitive or critical role whose key outputs depend upon processing information on a CL2 CIS system; or carrying out SECRET research and development activity.

Category B2. (Risk Impact Medium Low). Establishments holding assets or carrying out a role the loss, disruption or compromise of which would cause *damage* to the operational effectiveness or key business output of the TLB/TF or MOD.

For example:

Establishments, including branches of HQs, with a sensitive or critical role; or with a deployable operational role in a readiness cycle or having an essential force generation function; or whose key outputs depend upon processing information on a CL3 CIS system.

Category C1. (Risk Impact Low). Establishments holding assets or carrying out a role the loss, disruption or compromise of which would cause *difficulty* in maintaining the operational effectiveness or a key business output of the TLB/TF or MOD.

For example:

Establishments, including branches of HQs and units not included in Category A or B holding protectively marked information or equipment mainly at CONFIDENTIAL level or below with CL4 CIS systems that are not critical to key TLB/TF business or operational outputs.

Category C2. (Risk Impact Very Low). Establishments holding assets or carrying out a role the loss, disruption or compromise of which would cause *negligible damage* and would not significantly degrade the operational effectiveness or a key business output of the TLB/TF or MOD.

For example:

Establishments, including branches of HQs and units not in Category A or B that do not hold protectively marked information or equipment above RESTRICTED level or full bore weapons.

4. Categories P1-P3 relate to the threat to life posed by terrorism and retain agreed pre-SSR definitions used to determine guarding criteria. These definitions are contained in Section VIII to Chapter 5.

5. The process of categorisation of establishments is to involve an assessment of both the establishment's asset and guarding risk impact level, producing a combined value, e.g. B2/P1. Individual establishments and lodger units within a large site should be assessed according to their individual assets and vulnerabilities. For example, the perimeter and Service living accommodation on a large site may be designated P1 for threat to life reasons and include a sensitive unit that requires a Category A2 rating. This does not mean that each and every establishment within the site need be accorded the same Category A2 rating, regardless of the activities conducted within its own discrete area. Where there is a specific area within an establishment that requires a higher category, e.g. an operations or communications centre, it may be categorised separately from the remainder of the establishment which may then be placed in a lower category for inspection purposes.

Inspection Periodicity

6. Threats to Defence establishments vary widely, as do their vulnerabilities. Although every establishment should be subject to periodic formal security inspection, the programme should reflect these differences. In determining the frequency of inspections for establishments within their area, TLB Holders/TFCEs will need to consider various factors. These will include: the criticality of the establishment's output

in meeting MP objectives, the risk profile, the outcome of previous inspections and audits, turnover of key personnel and any mandated requirements. Security inspection reports will provide a major input into the DSO's annual Certificate of Assurance. TLB Holders/TFCEs may elect to supplement formal inspections by advisory visits and by the completion of security questionnaires. The guidelines for inspection periodicity are shown below:

Asset Category	Risk Impact Level	Inspection Periodicity (years)	Guarding Category		
			P1	P2	P3
			Inspection Periodicity (years)		
A1	High	1	3	4	6
A2	Medium High	2	3	4	6
B1	Medium	3	3	4	6
B2	Medium Low	4	3	4	6
C1	Low	5	3	4	6
C2	Very Low	6	3	4	6

7. It will be for TLB Holders/TFCEs to determine the detailed form of the inspections conducted, adjusting the emphasis of the inspection to take account of the importance of the establishment's outputs to the TLB/TF, its risk profile and security history. Whenever practicable, however, a security inspection should in principle be holistic in approach, taking due account of all relevant aspects of physical, personnel and information security, including the procedural measures taken to protect assets and CIS systems on the site concerned.

8. TLB Holders/TFCEs may opt to arrange inspections at more frequent intervals than given in the above matrix, in accordance with their risk management and resource decisions. If they elect to inspect establishments in a given category at intervals greater than the periodicity indicated in the matrix, TLB Holders/TFCEs will be required to provide an audit trail and rationale for the decision as part of the process of their reporting of security assurance and subsequent audit.

9. For many establishments, the guidance periodicity for asset and guarding categories will differ. It will be for TLB Holders/TFCEs to schedule the inspections programme so that both asset and guarding elements are inspected satisfactorily. As a guide, when asset and guarding category periodicities differ, the asset category periodicity should be taken as the driver for the conduct of comprehensive inspections, and the guarding category periodicity for supplementary inspections of relevant CT measures. For example TLB Holders/TFCEs might choose to schedule these additional

CT inspections around the mid point between comprehensive inspections. The following examples illustrate the options that are open to TLB Holders/TFCEs:

a. An establishment is categorised B1/P2, giving periodicity for inspections of 3 and 4 years. The TLB Holder/TFCE might choose to merge the two categories and carry out a combined inspection between the 3 and 4 year points. Alternatively, the TLB Holder/TFCE might choose to conduct all aspects of security inspection at the 3 year point, and carry out a supplementary CT-orientated inspection at the 4 year point.

b. An establishment is categorised C2/P2, giving periodicity for inspections of 6 and 4 years. The TLB Holder/TFCE might choose to adhere to the guideline periodicity, or to advance the CT inspection to the 3 year mid-point between holistic inspections.

This page intentionally left blank

ANNEX B TO CHAPTER 2

GUIDE TO THE CONTENTS OF SECURITY STANDING ORDERS

The headings given below are a guide to the items to be considered for inclusion, as appropriate, in security standing orders (SSOs). The list is not exhaustive as there are normally local matters to be included, nor is it intended to be a guide as to layout which should be arranged to enable parts to be issued as notices or for particular appointments.

Unit Security Organisation

1. Details of establishment security officers (showing name, establishment appointment and telephone numbers). Include details of any other officers with security responsibilities such as IT security officers and those responsible for overseeing the security aspects of contracts and contractors.

2. Include a general statement of their specific security responsibilities for:

   a. Control of arms, ammunition and explosives (including privately owned weapons such as shotguns).

   b. Safeguarding vehicles and equipment.

   c. Safeguarding protectively marked documents and material.

Control of Access

3. Control of access by:

   a. Gate controls.

   b. Passes and permits.

   c. Patrols and guards.

4. Handling of visitors, cleaners, contractors, public utility employees, and tradesmen.

5. Handling of trespassers.

6. Security area controls.

7. Key control.

8. Temporary vacation of offices.

9. Locking up and inspection of offices.

10. Operation of alarms.

Security of Information

11. Orders for and method of promulgation of:

    a. Establishment postal address.

    b. 'Need to know' principle.

    c. Security warnings.

    d. Use of copying and electronic equipment.

    e. Reporting of contacts with nationals of countries to which special security regulations apply and the intention to travel in these and certain other countries.

    f. Reporting suspicious incidents.

    g. Reporting of losses of identity cards, passes and permits.

    h. Reporting of rumours.

    j. Pen/tape friendships.

    k. Amateur radio activities including Citizen Band radio.

    l. Use of privately owned cameras in restricted areas.

    m. Communications with press and broadcasting organizations.

    n. Release of information.

Security of Communications

12. Telephone security.

13. Radio security (procedures, use of codes).

Security of Documents

14. Instructions for:

    a. Protected document registers (nominated and supervising officers).

    b. TOP SECRET control (if required).

15. Control of distribution, messenger service, and dispatch.

16. Removal of documents from offices, carriage of documents by hand at home and abroad with particular attention to the crossing of international frontiers by casual couriers with protectively marked documents.

17. Review, destruction, weeding and downgrading of documents.

18. Checks and musters of documents and files.

19. Reporting of and searching for missing documents, and action on loss or compromise of protectively marked documents.

20. Action to be taken on finding protectively marked documents.

21. Orders to be specially published to cover:

    a. Control of security containers, keys and combination lock settings.

    b. Minimum standards for the protection of protectively marked documents.

    c. Operation of duplicators and copying machines.

    d. Control of typing.

    e. Destruction of protectively marked documents and waste.

    f. Emergency destruction of documents.

    g. Ranks and appointments authorized to produce protectively mark documents.

Security of Weapons, Equipment and Material

22. Protection and inspection of weapons, protectively marked equipment and material.

23. Security of armouries. Control and issue of arms, ammunition and explosives, and orders for storage and movement.

24. Reporting loss, compromise or finds of protectively marked equipment, arms, ammunition and explosives.

Security of Information Technology Systems

25. Security operating procedures.

26. Physical security.

27. Technical security.

28. Document security.

29. Personnel security.

Security of Personnel

30. Maintenance of establishment vetting register.

Security Education and Training

31. Education of all ranks and civilian staff.

32. Training of clerical staff, protectively marked equipment storemen, and arms storemen in their security procedures.

Security on Exercises or Operations

33. Planning, organization, and briefing. (See also Chapter 14).

34. Restrictions on, and control of, protectively marked material taken on exercises or operations.

35. Security of information and documents, particularly:

a. During loading and unloading of office vehicles.

b. Guarding of documents.

c. Control of access.

d. Careless talk.

e. Reporting of suspicious incidents.

f. Searching of vacated areas.

g. Telephone security.

h. Radio security (procedures, use of codes).

36. Security of arms, ammunition and explosives.

Contracts Security

37. Security regulations for contractors. (See also Chapter 12).

This page intentionally left blank.

ANNEX C TO CHAPTER 2

SECURITY ORDERS, REGULATIONS AND INSTRUCTIONS FOR SECURITY OFFICERS

1. Security officers at all levels must acquaint themselves with current security directives. They must also be aware of the sources of reference and guidance on security matters contained in the publications detailed in this Annex. It is not expected that all of the publications will be held, but security officers should be aware of the existence of the documents.

2. Documents applicable to all security officers.

a. Queen's Regulations for the Royal Navy, Army or Royal Air force (as applicable).

b. Manual of Naval Law (BR 11) - Manual of Army Law or Manual of Air Force Law (as applicable).

c. JSP 440 - The Defence Manual of Security (DMS) Volumes 1 - 5.

d. Royal Navy, Army or Royal Air Force supplements (as applicable) to JSP 440.

e. Human Rights Act.

f. JSP 406 – Guidance to the Data Protection Act.

g. Defence Council Instructions and other administrative instructions (to include CONFIDENTIAL issues).

h. Technical Grading Committee lists.

i. Command and establishment security standing orders.

j. JSP 205 - Directory of Subscribers to Secure Voice Systems. (To be superseded by DCSA Publication 16 - BRAHMS/BRERE/STUII/STUIII secure speech systems.

k. Tempest regulations.

m. Table X - Release of UK Classified Military Information.

n. IDO regulations:

(1) C-M(55)15 (Final) - Security within the North Atlantic Treaty Organisation, Volumes I and II.

(2) C-M(64)39 - Draft agreement for co-operation regarding ATOMIC information.

(3) C-M(68)41 (5th Revise) - Administrative arrangements to implement the agreement between the parties to the North Atlantic Treaty on co-operation regarding ATOMAL information.

(4) C-M(71)27 (Revised) (including AC/35-WP/75) - Special Procedure for the Handling of US-SlOP Information.

(5) ACP 122 - Handling of ATOMAL Information within Classified Communication Centres, NATO supplement 2.

(6) CENTO/C/13D5 - Parts I to IV.

(7) AC/35-D/1006 (Revised) - Guidance on the Conduct of Inspections by NATO Component Security Authorities

(8) ACO 130 (Revised 1999) - Rules for the Handling and Release of Information Marked ATOMIC.

o. Other documents that may be specified in JSP 440.

3. Documents for Royal Navy security officers only.

a. BR 8988.

b. Ships Standing Orders.

c. BRN 01/17 - Manual of Naval Signals Intelligence.

c. FLAGOs.

d. Fleet Engineering Orders.

e. CB 03329 - Security of Classified Material.

f. Fleet Temporary Memoranda.

4. Documents for Army security officers only.

a. BWO 01/1 - Instructions for the handling of CRYPTO.

b. AGAIs (60974).

c. Div/District/Bde Standing Orders.

d. Unit Documentation Manuals.

5. Documents for RAF security officers only.

a. AP 3087; Manual of Security Education.

b. AP 3392; Manual of Personnel Administration.

c. PAM(Air) 58; A Guide to the News Media.

d. PAM(Air) 150; Introduction to Security.

e. CD 1167.

f. CD 1155; Communications Doctrine.

g. RAF GAls.

h. BAM/01/2; Instructions for the handling of COMSEC material in the RAF.

This page intentionally left blank.

ANNEX D TO CHAPTER 2

SECURITY INCIDENTS - MANDATORY REPORTING TO MINISTERS

Scope

1. There is a requirement to staff reports on security incidents to Ministers in an accurate and timely way to ensure that security incidents which might attract public, Parliamentary or media attention are brought to their notice. This instruction identifies which types of incident are to be reported and the methods to be used. Advice can be sought at any stage from the appropriate TLB/Chain of Command, who should be informed immediately that an incident has occurred.

Types of Security Incident

2. Security incidents falling into any or all of the following categories are to be reported to Ministers:

a. Incursions onto MOD sites which involve a significant[1] threat to the security of the unit or establishment. (e.g. if a significant asset is compromised, even if temporarily).

b. Incursions onto MOD sites where there has been a significant failure of security measures.

c. Incursions which are likely to attract media, public or parliamentary attention.

d. Any incident where espionage, terrorism or sabotage is thought to have been involved (except in NI, where procedures laid down in CDS's Directive to GOC NI will be followed (i.e. incidents are reported in a dual system, firstly to MO2 by HQNI G3 (Ops) and then relayed up the Chain of Command as necessary and additionally by either HQNI, Sec(HSF)3 or D Policy to Ministers, verbally in the first instance with a follow-up written report if required by Ministers' Private Offices, with D Def Sy as an information addressee.

e. All losses or theft of arms/explosives or significant quantities of ammunition.

[1] It is not possible to define "Significant" more specifically. It is a matter of judgement but advice may be sought from the appropriate TLB PSyA/Chain of Command Security Staff or D Def Sy.

f. Any loss or theft of information where there is likely to be media, public or parliamentary interest, or embarrassment to the Department.

g. All leaks of official information.

h. All instances of intrusion into or malicious electronic attack on MOD IT Systems from external sources.

j. All instances of intrusion into or malicious electronic attack on MOD IT Systems from external sources.

k. All instances where significant damage results from the destruction or corruption of information on MOD IT Systems, as a result of malicious software e.g. viruses, worms or trojan programmes.

l. Personnel security cases where there is likely to be media, public or parliamentary interest, or embarrassment to the Department. (In many incidents the personnel security aspect will not become apparent until an investigation is under way and it is likely therefore that the incident will initially fall within one of the criteria described above).

Responsibilities

3. Responsibility for staffing reports to Ministers rests with the TLB/Chain of Command which should take the lead consulting, as necessary, the Security Staff and Civil Secretariats which must also be involved, and D Def Sy. (The exception to this is HQ LAND where the Command Secretary will lead). However, the following exceptions to this staffing arrangement apply:

a. Northern Ireland. Civil Secretary HQNI or Sec HSF 3 (consulting MO2 as necessary).

b. Nuclear Security. The TLB/Chain of Command responsible is to make the report except for the specific areas of nuclear security below:

(1) Nuclear Weapon/Material Movements (including incidents at staging posts - D Nuc Pol/AD NAR.

(2) Nuclear Assets at Sea (i.e. out of port) - NS(Sec).

(3) AWE – DPA NW IPT.

It should, however, be noted that separate reporting instructions are set out in JSP 440 Volume 4 covering Terrorist threats to nuclear assets, under Codeword BINGHAM and where such incidents have a safety dimension additional reporting under Codewords TOPSTAR, PRIMROSE or LIABLE remains unchanged.

c. Security at USAF Bases in GB. DAS 3b(Sec).

d. MOD Police Operations and Organisation. The MDP is not a Security Authority, but when security incidents involving MDP personnel take place, the reporting TLB/Chain of Command is to liase with MDP Secretariat to ensure that the MDP involvement is fully covered. Early liaison with the MDP Secretariat will ensure that only one Ministerial submission is prepared. MDP Sec is equally responsible for liaison with the appropriate TLB/Chain of Command before making a Ministerial submission.

e. Security Involving Defence Contractors (List X). D Def Sy.

f. Personnel Vetting Cases. CE/DVA. DVA will consult PSyAs and Security Staffs and Secretariats who may lead if the decision on a case was taken outside the DVA.

4. Any cases of doubt regarding responsibility should be referred to D Def Sy in the first instance.

Procedures

5. In order to alert the security system that an incident has occurred and to provide subsequent monitoring of it, there are four steps outlined below which are to be followed. D Def Sy is to be an information addressee on all reports/submissions and is able to provide advice at any stage of an incident or during the reporting process.

Step 1: Initial Report

6. An initial report, usually by telephone, is to be made to MOD as soon as is practicable after a security incident. This will allow early notification of Ministers and appraisal of the degree of importance of the incident to take place. TLBs/Chain of Command should decide who should make this report; however reports should not be delayed. This is particularly important in the case of a major incident (e.g. a terrorist attack or large incursion to an establishment). Contact details are:

General Incidents (terrorism, extremism, espionage etc)

Working hours: D Def Sy Phys (Non Tech/Threats), MB 84815/020 7218 4815.

Out of hours: CDSDO, MB 88850/020 7218 8850.

Documentary Losses

Working hours: D Def Sy InfoSy (Pol)1, MB 83994/020 7218 3994.

Out of hours: CDSDO, MB 88850/020 7218 8850.

IT Incidents

Working Hours: D Def Sy InfoSy (Tech), MB 84505 or 87811/020 721 84505 or 87811.

Out of hours: Duty IT Sy Officer Via MDP 01371 85 4444.

Nuclear Weapons/Material Movements

During Moves: D Nuc Pol/NAR Ops, MB 86763/020 7218 6763.

During Overnight Stops at Staging Posts: CDSDO, MB 88850/020 7218 8850.

7. The initial report is to be followed as soon as possible by a written report, normally by signal, in the format at Annex H. The relevant TLB/Chain of Command is to decide whether this is sent by the unit/establishment concerned or by the TLB HQ.

Step 2: Ministerial Submission

8. Ministerial submissions should normally be made within 24hrs and are to expand on the information given in the initial written report. They should be made direct to PS/Minister(AF) and copied to:

APS/SofS	}	
PS/PUS	}	All incidents.
DGS&S	}	
D Def Sy	}	
PS/Minister(DP)	Where the Defence Procurement Agency is involved.	
PS/2nd PUS	Where civilian staff are involved.	
MA/DCDS(C)	Where operational matters are concerned.	
D Nuc Pol	Where nuclear facilities/materials/weapons are involved.	
ACNS and NS(Sec)	}	

ACGS via ASD 1	} Where single Service matters are concerned.
ACAS and DAS 3b Sec	}
MA/CDL	Where DLO matters are concerned.
CCMDP	Where MDP officers are involved or based.
D News	All incidents (sensitive details may be excluded).

Step 3: Progress Reports

9. Progress reports may be required, depending on the seriousness of the incident and directions given by Ministers following the initial report. D Def Sy will agree with the TLB/Chain of Command concerned whether these are needed, at what frequency they should be submitted and their distribution. This process will ensure that lessons from any incident are identified as early as possible and used to amend or develop policy and/or procedures. It will also ensure that Ministers are kept fully informed.

Step 4: Final Report

10. A final report may be submitted once the incident is closed and following discussion between D Def Sy and the TLB/Chain of Command concerned. This may take the form of a submission to Ministers, depending on the outcome of the investigation. It should include any specific recommendations for alterations to security policy or procedures arising from the investigation of the incident.

This page intentionally left blank

ANNEX E TO CHAPTER 2

SECURITY INCIDENTS - MANDATORY REPORTS TO MINISTERS - INITIAL REPORT SIGNAL FORMAT

(Text in *italics* is for completion by originator)

From: *Unit/ establishment or TLB/Chain of Command HQ*

To: MODUK

Info: *Chain of command(including PSyA and Security Staff)*

Others as required

SIC: YAL/Y2G

Precedence: IMMEDIATE

Protective Marking: RESTRICTED (as a minimum)

SECURITY INCIDENT – INITIAL REPORT

1. *Date, time and place of incident*.

2. *Brief details of incident.*

3. *Persons/property involved (if known).*

4. *Organisation(s) conducting the investigation*.

5. *Presentational aspects, including known media interest and suggested lines to take.*

6 *Any immediately apparent conflict with extant security policy.*

7. *Expected date/time of submission to Ministers.*

8. *TLB/Chain of Command POC.*

This page intentionally left blank

ANNEX F TO CHAPTER 2

FORMAT OF IMMEDIATE SIGNAL REPORT OF SUSPECTED LOSS OR COMPROMISE OF PROTECTIVELY MARKED MATERIAL

The report is to state:

a. What has been lost.

b. Its protective marking (including caveats and descriptors).

c. Its originator or sponsor, date of origin, reference number, title or subject and copy number.

d. An assessment of whether compromise is certain, probable, possible or unlikely. PSyAs or Command security staff will inform the sponsor in order to obtain an assessment of the effect of compromise.

e. Although the major cause of losses is carelessness, the reporting officer may nonetheless, by virtue of his inquiries, have formed an opinion that espionage or subversion is or may be involved. When this is the case, or where no further action is intended, a brief summary of circumstances surrounding the loss is to be given, together, where appropriate, with the full names and service or staff numbers of those involved. Where names are given the signal is to be protectively marked at the appropriate level and is to include the descriptor STAFF.

f. Corrective measures to prevent a recurrence (if appropriate at this stage).

g. Whether or not further action is intended.

This page intentionally left blank.

CHAPTER 3

RISK MANAGEMENT

This page intentionally left blank

CHAPTER 3

RISK MANAGEMENT

General

0301. Risk management provides the method for conducting the protective security process. It is the means to ensure that the security measures adopted to counter the threats posed to assets reduce the likelihood of compromise to an acceptable level but are not greater than are warranted by the asset's value. It is a common sense methodology to enable the selection of appropriate and cost effective security measures. The main elements are:

a. Deciding what assets need to be protected and how valuable those assets are.

b. Deciding what threats are posed to the assets and how vulnerable they are to them.

c. Reviewing and adapting existing security measures to ensure that they:

(1) Meet mandatory security requirements known as baseline measures.

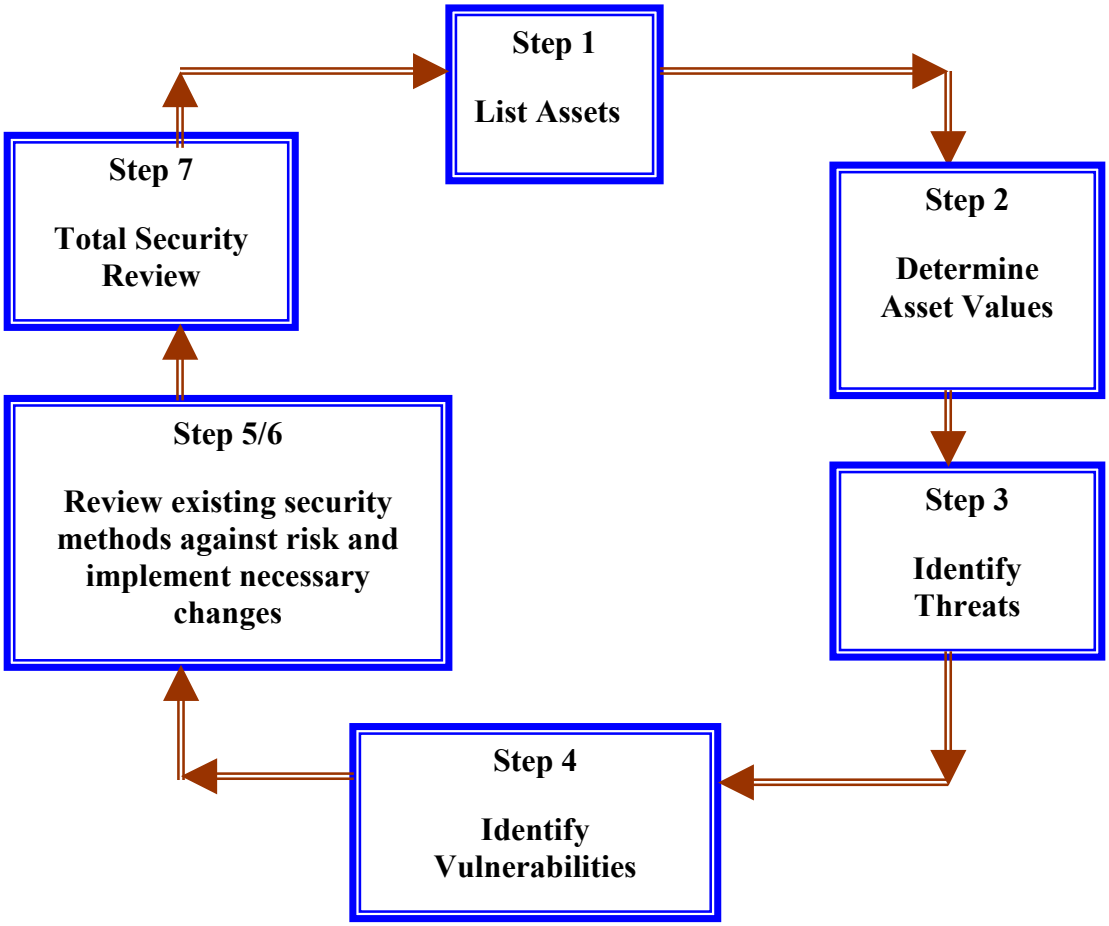
(2) Provide an acceptable level of risk that compromise will not take place.

d. Examining overall security procedures on a regular basis to make sure that they provide a sensible and economic interrelationship.

e. The process is to be documented at establishment level and the records retained so that any future changes to asset values, vulnerabilities and threats can be accommodated.

The Theory of Risk Management

0302. The theory of risk management is shown below:



Risk Management Practice

0303. The following is an explanation of the steps given in the above diagram:

a. **Step 1. List All Valuable Assets.** The risk management methodology can be applied to any asset to which the HOE attaches value. These could be information, physical assets and even peoples' expertise. It is mandatory for these assets to be listed in the manner shown at Annex A:

(1) **Information.**

(a) Protectively marked documents. (Document, as defined in the Glossary, includes maps, view foils, IT storage media, etc).

(b) Equipment that merits protective marking for confidentiality.

(c) IT systems giving access to protectively marked information. In addition to requirements for protecting the information, as such, these will also require protection as physical assets. They are subject to approved system security policies (SSPs) and security operating procedures (SyOPs). Further detail is in Volume3. Information Technology.

(2) **Physical Assets**

(a) Arms.

(b) Ammunition.

(c) Explosives.

(d) Dangerous drugs.

(e) Toxic substances.

(f) Public funds.

(g) Any physical asset the compromise of which would cause serious damage to the operational effectiveness of the establishment e.g. aircraft, ships, AFVs or an essential IT system or command and control centre.

(3) **People**

(a) Service personnel and MOD employees working in the establishment.

(b) Dependants living within the establishment.

(c) Visitors to the establishment (e.g. students attending courses or contractors working on a project).

b. **Step 2. Determine Asset Values.** Using the protective marking definitions at paragraph 0103 of Chapter 1 decide the protective marking

category for each asset taking into account compromise of confidentiality, integrity and availability. Consider both the **direct** and **indirect** consequences of compromise. Where there are a number of assets of the same type and protective marking, take into account their aggregated value, e.g. Would the information contained in a large number of CONFIDENTIAL documents, held in a single file, require the protective marking of SECRET if that information was condensed into a single document? Physical assets which require to be listed (e.g. arms, ammunition and protected equipment) are unlikely to carry protective markings but must be treated, for security purposes, as though they were protectively marked.

c. **Step 3. List both Types and Levels of Threat.** Against each asset group (such as information) list the type(s) of threat (e.g. espionage or theft) and the threat level as defined in Annex D to Chapter 1 or in the case of terrorism Annex E to Chapter 1. An example of a completed record that might be made by an establishment for Steps 1 to 3 of the Risk Management Process is at Annex B.

d. **Step 4. Identify the Vulnerability of Assets.** Consider any vulnerabilities of the asset itself e.g. that it radiates sensitive information and is therefore vulnerable to intercept. Also consider vulnerabilities in the existing security arrangements. Usually this will be carried out with the assistance of professional security personnel. Aspects to be considered include:

(1) Perimeter security e.g. access control and effectiveness of security fences.

(2) Internal security e.g. intruder detector systems (IDS), security furniture, procedures such as the disposal of protectively marked waste and arrangements for the movement and storage of arms, ammunition and explosives.

(3) Personnel security e.g. escorting of visitors and vetting and supervision of relevant staff.

(4) Communications and technical security e.g. security of photocopiers and computer systems.

e. **Step 5. Review existing Security Counter-measures for Confidentiality and implement necessary changes to achieve Baseline Measures.**

(1) **Stage 1.** For all assets where **confidentiality** is a concern it is necessary to apply any measure required to achieve the security standards set out at Annex A to Chapter 1. In order to achieve a common and acceptable standard of protection throughout the Government Service at each level of the protective marking system, certain baseline measures are mandatory. The following baseline measures are to be applied when confidentiality is at stake:

(a) **Universal Baseline Measures.** These are the general preventative measures that form a normal part of good management practice e.g. implementing relevant health and safety legislation. A list of universal baseline measures is at Annex C.

(b) **Control and Carriage Baseline Measures.** The mandatory standards for the control and carriage of protectively marked assets are given throughout Chapter 4 and at Annex C to Chapter 4. As these baseline measures are set for a "Low" threat, it may be necessary to add additional measures if the threat is higher than "Low".

(c) **Physical Security Baseline Measures.** The mandatory standards for the physical protection of assets are arrived at by following the matrix of options and menu of measures at Annexes A and B to Section 1 of Chapter 5.

(d) **Counter-eavesdropping Baseline Measures.** The mandatory standards for protection against eavesdropping are covered in Chapter 27 of Volume 3.

(2) **Stage 2.** Having noted the relevant baseline measures and standards of security, review existing security counter-measures and decide if they are excessive, adequate or inadequate in relation to the threat. If excessive, consider whether funding or resources can be saved by reducing them sensibly while still maintaining the desired level of security. If wholly adequate, do no more. If inadequate, then the assets are at an unacceptable degree of risk. A decision is required on what to do to reduce the risk to an acceptable level. This may be achieved by either introducing suitable counter-measures to bring the level of security up to the baselines or by reducing the risk in some other way such as transferring the most valuable assets to a site with a higher degree of security.

f. **Step 6. Review existing security counter measures for integrity and availability and implement necessary changes to achieve mandatory standards.**

(1) **Stage 1.** For all assets where **integrity** or **availability** are a concern, it is necessary to consider how to achieve the standards of security set out at Annex A to Chapter 1 as they can be related to the value of the asset. In order to achieve a common and acceptable level of protection the following standards are mandatory:

(a) **Universal Baseline Measures.** The universal baseline measures at Annex C are to be applied.

(b) **Arms, Ammunition and Explosives.** The mandatory requirements for the protection of arms, ammunition and explosives given in Chapter 5 are to be applied.

(c) **Nuclear Assets.** The mandatory requirements for the protection of nuclear assets given in the Defence Manual of Security Volume 4 are to be applied.

(d) **Dangerous Drugs, Toxic Substances and Public Funds.** Those mandatory security requirements for the protection dangerous drugs, toxic substances and public funds that form part of current, MOD or single-Service instructions are to be applied.

(2) **Stage 2.** Having noted the relevant baseline and mandatory levels and standards of security, review existing security counter-measures in the manner described at para 0303e(2) above and take action accordingly. In some cases the measures designed to protect confidentiality may provide or contribute to protection for integrity and availability. However, usually integrity and availability can best be safeguarded by making suitable contingency plans e.g. by making regular backup copies of information vulnerable to loss of availability. Where an asset has a clear monetary value, cost benefit analysis techniques will help to decide how much it is worth spending to protect it.

g. **Step 7. Total Security Review.** Conduct a general review of counter-measures against threats and vulnerabilities to ensure that the overall result meets mandatory standards, is cost effective and that the HOE is prepared to accept any remaining residual risk. Also ensure that the key facts

and decisions in the risk management analysis have been recorded to enable audit in the future.

0304. Follow Up Action. Risk management is an ongoing process. The ingredients: asset values, threats, vulnerabilities, risks counter-measures and the degree of risk that is acceptable do not remain static. The risk may vary over time requiring changes in protective security. Any risk management process must therefore be sensitive to changes and should be reviewed by the ESyO whenever a significant change takes place and annually.

This page intentionally left blank

ANNEX A TO CHAPTER 3

Record for Steps 1, 2 and 3 of Risk Management Process

Asset group/type	Asset (Note 1)	Value (Note 2)			Quantity (Note 3)	Listing (Note 4)	Location (Note 5)	Aggregate Value (Note 6)			Threat type/level (Note 7)
		C	I	A				C	I	A	
Information											
Documents											
Equipment											
IT Systems											
Physical											
Arms											
Ammunition											
Explosives											
Dangerous drugs											
Toxic substances											
Public funds											
Operational effectiveness											
People											
MOD employees											
Dependants											
Visitors											

Notes on completion of record for steps 1, 2 and 3

1. **Note 1 - Asset.** List assets in general terms under the appropriate asset type heading, for example the "Arms" asset type might show just 2 entries "small arms" and "support weapons". In the case of documents it is only necessary to show "TOP SECRET", "SECRET", "CONFIDENTIAL", "RESTRICTED" if documents with any of those protective markings are held. For IT systems state only the project name and PC for personal computers.

2. **Note 2 - Value.** Show the protective marking for each asset under the appropriate headings of Confidentiality (C) Integrity (I) Availability (A). In the case of documents or other material, it is probable that only the 'C' column would be completed, where as for equipment or IT systems the 'I' and 'A' might have a protective marking value. For example although an IT system might only store information protectively marked up to RESTRICTED, the damage that might arise following the corruption or non availability of vital data might warrant a higher protective marking under 'I' and 'A'. Unless physical assets have an aspect of confidentiality such as a weapon that is CONFIDENTIAL, their value should be recorded under 'A'. All arms, ammunition, and explosives are to be allocated the protective marking SECRET, unless such as in the case of nuclear weapons their value might be TOP SECRET.

3. **Note 3 – Quantity.** State only the approximate quantity e.g. for CONFIDENTIAL DOCUMENTS – '200-250' or an IT system – '12 Terminals'.

4. **Note 4 – Listing.** State the register in which the assets are recorded if a record is held. In the case of SECRET or TOP SECRET protectively marked documents, equipment and material show 'MOD Form 102' and relevant volumes. As CONFIDENTIAL and RESTRICTED are not recorded state 'Not Recorded' for any such holdings. Likewise for Physical Assets, give the record if one is kept such as 'Arms Register'.

5. **Notes – Location.** Give a very general statement of where the asset is normally held or worked upon e.g. for Arms – 'Armoury' or RESTRICTED documents – 'all buildings'.

6. **Note 6 – Aggregate Value.** If the compromise of the full collection of assets of a particular type would cause greater damage than the compromise of a single asset, state the aggregate value under the headings Confidentiality (C), Integrity (I) and Availability (A). For example, the compromise of the total holdings of SECRET documents might cause damage in confidentiality to the value of TOP SECRET. If the aggregation of items would not increase their compromise damage from that shown in the value column, enter the same protective markings as that of the Value column.

7. **Note 7 – Threat Type/Level.** Insert threat type e.g. Theft and level e.g. MODERATE. Guidance for threat levels can be found in Annexes C, D and E to Chapter 1.

ANNEX B TO CHAPTER 3
RECORD FOR STEPS 1, 2 AND 3 OF RISK MANAGEMENT PROCESS - EXAMPLE

Asset group/type	Asset (Note 1)	Value (Note 2)			Quantity (Note 3)	Listing (Note 4)	Location (Note 5)	Aggregate value (Note 6)			Threat type/level (Note 7)
		C	I	A				C	I	A	
Information											
Documents	TOP SECRET	TS			2	MOD F102 Vol 1	Strong room	TS			Espionage/Low
	SECRET	S			12	MOD F102 Vol 1-4	(Strong room (2IC office (Int cell	S			Leaks/Med
	CONFIDENTIAL	C			40-60		HQ building	S			Theft/Med
	RESTRICTED	R			500-600	Not listed	Most buildings	R			Data Corruption/ Med
						Not listed					
Equipment	Ptarmigan	C		C	5 Sets	MOD F102	Building 3	C		C	
IT Systems	CASH	S	C	C	1 Terminal	IT REGISTER	HQ building	S	C	C	
	UNICOM	R	R	R		-"-	HQ building	R	R	R	
	PCs	R	R	R	5 Terminals	-"-	HQ+bldg 5 & 7	R	R	R	
					21 Terminals						
Physical											
Arms	Small arms	-		S	650-700	Arms Register	Armoury			S	Theft/Low
	Support wpns			S	25-30	Arms Register	Trg			S	
Ammunition	Small bore			S	250-270K		Ammo Store			S	
	All natures			S	6-7000	Ammo Register	Ammo Store			S	
Explosives	PE			S	10-12 lbs	Ammo Register	Explosives Store			S	
Dangerous drugs	Drugs		-	C	small	Explosives Register	Med Centre			C	
	None			-	-						
Toxic substances	Funds			R	£3-4K	MO Register	HQ Building			R	

Asset group/type	Asset (Note 1)	Value (Note 2)			Quantity (Note 3)	Listing (Note 4)	Location (Note 5)	Aggregate value (Note 6)			Threat type/level (Note 7)
		C	I	A				C	I	A	
Public funds Operational effectiveness	 AFVs B Vehicles		 C R	 C R	 101 71	 AB 562 MT MT	sub-unit offices Vehicle Park Vehicle Park		 S C	 S C	
People											
MOD employees Dependants Visitors	Individuals working in establishment Individuals living in establishment Individuals visiting establishment				850-875 250-275 30-50	UNICOM UNICOM Guardroom register	2xMesses Accn blocks A&B Jnr Ranks Club Offices			N/A N/A N/A	Terrorism/Low

ANNEX C TO CHAPTER 3

UNIVERSAL BASELINE MEASURES

1. MOD organizations must comply with all relevant legislation including:

   a. All health and safety legislation.

   b. All fire acts.

   c. All relevant building acts.

   d. Any legislation concerned specifically with the safeguarding of information and assets.

2. MOD organizations are to comply with current counter terrorist guidelines, appropriate to the terrorist threat.

3. MOD organizations handling protectively marked information must adhere to interdepartmentally agreed technical standards where relevant, such as in computer and communications security.

4. MOD organizations are to take all reasonable steps to ensure that security considerations are taken into account in the design of information systems.

5. MOD organizations are to respect all international obligations to protect assets to a required level.

6. MOD organizations are to take reasonable steps to ensure that new buildings are designed to reach reasonable standards of security and that the same standards of security are achieved when existing buildings are adapted. (The appropriate British standards provide useful guidance).

7. MOD organizations are to ensure that all valuable assets are kept in environmentally suitable conditions.

8. MOD organizations are to ensure that all staff receive adequate education in the application and relevance of protective security measures and in their own protective security responsibilities in order to raise their level of awareness of the importance of security issues.

9. MOD organizations releasing protected assets outside Government service must ensure that the assets concerned are at no greater risk than if they were being

held by a Government department or agency. The conditions necessary to satisfy this requirement must form part of a contract or be included in a legally binding confidentiality agreement.

10. MOD organizations are to ensure that those handling protected assets are made aware of the level of protection required. Usually this will be by marking the asset but sometimes this may not be possible. Where protected assets are released outside Government service, holders must also be given guidance about how to achieve the required level of protection.

11. MOD organizations are to consider the need for a contingency plan in the event of an emergency.

12. MOD organizations are to ensure that people are accommodated and work in conditions which protect them from any likely threat.

CHAPTER 4
CONTROL AND CARRIAGE OF PROTECTED DOCUMENTS

CHAPTER 4

CONTROL AND CARRIAGE OF PROTECTED DOCUMENTS

SECTION I

CONTROL OF DOCUMENTS

General

04001. Universal baseline measures. The following are universal baseline measures:

a. Protectively marked documents must be produced, handled and reproduced only by persons with authorized access to the information they contain. Care must be taken to apply the "need to know" principle in the preparation, processing and distribution of protectively marked material. It is particularly important that copies are to be limited to those persons with a "need to know".

b. The protective marking on any asset must be conspicuous so that its value is readily apparent.

c. The protective marking is given to an asset by the originator and it may not be changed without the originator's authority. This applies equally to UK assets and those originating from foreign governments or organisations.

d. Assets sent overseas to UK posts, foreign governments, or other organisations are to be protected in accordance with the originator's marking and, additionally, care must be taken where appropriate to protect it from disclosure under any freedom of information (FOI) legislation by the use of national caveats and other special handling instructions.

e. Assets received from overseas posts, foreign governments or other organisations must also be protected in accordance with the originator's marking.

f. No "originator's copy" of a protectively marked document in any media may be destroyed unless it has been determined by the Desk Officer that it has no historical or research value (JSP 441 - The Defence Records Management Manual refers).

Note: Physical protective measures for documents, including those in transit and at temporary locations, are referred to in this Chapter but are given in more detail in Chapter 5.

04002. Responsibilities of heads of establishment(HOE). HOE are responsible for:

a. Ensuring effective supervision when protected documents are being handled.

b. The correct creation, reproduction (by whatever means and in whatever form), receipt, despatch or disposal of such documents and their control.

c. Ensuring that, where called for by these regulations, such documentation is correctly recorded in protected document registers (PDR)(MOD F 102, or equivalent).

Preparation of protectively marked documents

04003. General. The protection to be afforded to a document is to be indicated by a series of markings which conveys how that document is to be handled. The agreed order of markings is: PROTECTIVE MARKING/DESCRIPTOR/STRAP VALUE/CODEWORD/NATIONAL CAVEAT. Such markings are to be centred and placed at the top and bottom of each page. They should be in larger or bolder print or stamped. Overstamping is not required. The following regulations apply to all protectively marked documents. Additional requirements generated by special rules, eg Caveats, will be dealt with in the appropriate sections of this manual. The creation and distribution of TOP SECRET and SECRET information on IT systems may differ from the procedures for paper based documents and is covered in detail in JSP 440 Vol 3.

04004. Baseline measure. The following are baseline measures:

a. Each SECRET and TOP SECRET document is to bear the title of the originating office, a reference number and date of origin. Any protectively marked documents issued in a series are to be serially numbered.

b. All TOP SECRET, TOP SECRET (CODEWORD or CAVEAT) documents and SECRET publications are to be copy numbered. Where appropriate, copy numbering is to be done at once.

c. Each page of a SECRET or TOP SECRET document is to be numbered. Each SECRET or TOP SECRET appendix or annex is to be page numbered in a separate series. (Although not a Baseline measure it is best practice to show the total number of protectively marked pages at the front of a document).

d. It is best practise that any protectively marked document that is likely to be amended is to include an amendment record sheet in the format shown in Fig 1.

AL No and Date	Authority	Date of Insertion	By Whom Amended	Independent Checker

Fig 1 Amendment Sheet

e. Originators of multi-page documents, whose overall protective marking is SECRET and above, should, where possible, show the protective marking for each individual paragraph. The protective marking should be shown at the end of each paragraph using the first letter of the appropriate marking eg (R), (C), (S) or (TS). Caveats, descriptors etc that are also applicable to individual paragraphs are to written in full eg (C-UK EYES ONLY), (S-STAFF) etc.

04005. Responsibilities. Those originating or authorizing the production of protectively marked documents, or authorizing subsequent reproduction or printing, are responsible for ensuring the maintenance of proper security during those processes. Where originators consider document protection justifies tighter control, the words "No copy to be taken without reference to and agreement by [the originator]" should be included below the protective marking and descriptor/caveat/codeword. HOEs/ COs/Directors shall delegate authorization for the production or reproduction of protectively marked documents to those persons within their organisation whom they deem to be sufficiently experienced and reliable to ensure that adequate control of security procedures is maintained.

04006. Originators of protectively marked documents which are issued against standard distribution lists must ensure:

a. All addressees have a continuing need to know.

b. All addressees have been correctly identified.

c. The above should be achieved by periodic review - at least once a year.

d. TOP SECRET documents are never to be issued on a standard distribution list.

Copy numbering of reproduced documents

04007. Reproduced copies of all TOP SECRET documents, and SECRET documents bearing copy numbers, are to be marked:

"Reproduction copy No.... of ....".

Establishments authorizing reproduction are responsible for adding numbers to individual copies provided by a reprographics pool or using in-house facilities: they are also responsible for ensuring that original documents and copies taken are accounted for in accordance with the relevant regulations (see separate instructions for IDO material).

Security warning notice

04008. A security warning notice is to be placed on all manuals, works of reference or sets of instructions, etc (but not on correspondence) marked RESTRICTED and above and reading as follows:

> "THIS DOCUMENT IS THE PROPERTY OF HER BRITANNIC MAJESTY'S GOVERNMENT, and is issued for the information of such persons only as need to know its contents in the course of their official duties. Any person finding this document should hand it to a British forces unit or to a police station for its safe return to the MINISTRY OF DEFENCE, (DDefSy), ST GILES COURT, 1-13 ST GILES HIGH STREET, LONDON WC2H 8LD with particulars of how and where found. THE UNAUTHORIZED RETENTION OR DESTRUCTION OF THE DOCUMENT MAY BE AN OFFENCE UNDER THE OFFICIAL SECRETS ACTS OF 1911-89. (When released to persons outside Government service, this document is issued on a personal basis and the recipient to whom it is entrusted in confidence, within the provisions of the Official Secrets Acts 1911-89, is personally responsible for its safe custody and for seeing that its contents are disclosed only to authorized persons)."

Authorization for reproduction of protectively marked documents

04009. Documents marked SECRET or above which are to be typed or reproduced require a full audit trail, this can be achieved by the use as appropriate of MOD F 72, MOD F 24 or MOD F 102. The authority for reproduction must be signed by officers with the appropriate delegated authority. Originator's approval must be obtained before reproduction of TOP SECRET or copy-numbered SECRET publications. Copies produced are to be numbered in accordance with the relevant regulations.

04010. If MOD F 72 is being used, Part A of the completed form will be returned with the completed work for retention with its duplicate for at least five years. Parts B and C (as appropriate) will be retained for six months by the typing and/or reproduction pool with the record of work done.

Registration and filing

04011. Baseline measure. All TOP SECRET and SECRET documents and files need to be registered and placed as soon as possible in serially numbered files or containers. The movement of SECRET and TOP SECRET material whether

internal, incoming or outgoing to a department or agency, must be recorded.

04012. Documents protectively marked SECRET or above must:

a. Be traceable at all times.

b. Be handled by as few people as possible and access to them restricted to personnel having a need to know.

c. Have the number of copies produced, in whatever medium:

(1) Recorded (see para 04013).

(2) Kept to the absolute minimum.

(3) Be segregated from unclassified material where this is practical.

Recording location, movement and disposal of protected documents

04013. Recording protected documents. A record is to be kept of the creation, reproduction, receipt, despatch, movements or disposal of all documents marked SECRET or above:

a. Records are to be kept in protected document registers (PDR) (MOD F 102 or equivalent) maintained in establishments.

b. Where convenient, PDRs can be kept in private offices and in any branch or section separate from the parent organisation. In this event, PDRs are to be registered with the parent Registry custodian so that the necessary independent checks of protectively marked material required in paras 04044 -04054 are comprehensively carried out.

c. All incoming documents with receipts attached must be page checked before receipt is acknowledged.

d. **Dispensation for not recording documents.** In very exceptional cases, where large quantities of protected documents are held or worked upon and where managers could achieve significant savings by establishing secure zones within which the recording of protected documents could be abandoned, a request for dispensation for not recording documents may be submitted to the appropriate Principal Security Adviser for consideration. The request for dispensation should include a full description of physical and procedural compensating measures, either in place or proposed, which would ensure the continued security of the documents to the appropriate standard.

04014. PDRs (MOD F 102) are to show by date of registration:

a. The appointment of the originator/sender, the date of origin, reference, copy number (if any), title (or subject) and protective marking of the document.

b. If the item is retained within the area served by the registration point, "final disposal" details must give the reference of the file, folder, filing box or library together with the enclosure/folio number.

c. Particulars of receipts (MOD F 24, etc) and, if appropriate, details of destruction, are also to be shown.

d. The temporary location of a loose document marked SECRET or above circulated within an organisation (under cover of a document location slip [MOD F 1 or equivalent]) prior to filing must be shown in the PDR with the appointment or name of the officer currently holding it.

e. PDR entries must be completed at the earliest possible opportunity by recording the final disposal of documents.

04015. Regular, efficient inspections of PDRs constitute a principle safeguard of document security. They identify inaccuracies, omissions or outstanding items in good time for them to be rectified:

a. PDRs are to be inspected by a nominated supervising officer at least once a month to ensure that they are being maintained correctly.

(1) The front page of the PDR provides space for the supervising officer to be identified and record the inspections.

(2) In establishments where details of protected documents are recorded/retained on computer systems, similar checks are required to ensure completeness of the entries through the production of monthly printouts. Supervising officers should record their inspection separately.

b. PDRs are also to be subject to periodic spot checks under local arrangements. PDRs are not considered "closed" until final disposal details are included for all entries and, where appropriate, receipts obtained for documents. In Service establishments, PDRs are not considered to be "closed" until all entries have been "red-lined" indicating the destruction or downgrading of the document or its transfer to another register. Closed PDRs must be retained by the registry for at least five years.

04016. Filing protected documents. All protectively marked papers are to be placed on files with the minimum of delay.

a. Protectively marked documents which require to be circulated (eg as float copies) should be enclosed in suitably marked colour-coded folders appropriate to the contents.

b. Such documents should not be retained by officers until they have been correctly and permanently filed.

c. Files containing protectively marked documents not currently in action should be returned to, and held in, the appropriate registry.

d. Should any enclosure/folio be removed temporarily from a file, a note is to be placed on the file identifying the document by its reference, date, originator and subject and giving details of its temporary location.

e. Enclosure/folio numbers and particulars of all TOP SECRET and SECRET documents (together with details of any protectively marked attachment, annex etc) are to be recorded on an enclosure/folio sheet placed inside the front of the file cover. MOD F 672 has been designed for this purpose. An example is at Annex A.

04017. All documents marked SECRET or above which cannot be placed on a file because of size or the nature of the material (eg books, computer tapes, films and transparencies) are to be:

a. Traceable through PDR entries or RN CB Form R.

b. Either placed inside numbered, or otherwise identifiable, folders, filing boxes or library bearing the appropriate protective marking or, if this is impracticable, should themselves be marked with an identifier which corresponds to the entry in the final disposal column of the PDR.

c. Housed in a security container of appropriate standard.

04018. Spare copies. Spare copies of protectively marked documents, including float and book copies, require as much protection as the originals and should be kept to a minimum. The requirement for the spare copies is to be reviewed not less frequently than once a quarter with a view to destruction. Spare copies are not to be made of TOP SECRET documents.

04019. Amendments to protected documents are to be incorporated into the document by authorised personnel as soon as possible after receipt. It is of vital importance that extreme care is taken when amending protected documents of looseleaf format. It is best practise that the following checks are carried out:

a. On receipt of an amendment, it is to be checked for completeness before it is incorporated in the document it relates to;

b. After incorporation of the amendment, the person who has made the amendment should:

(1) Check the document against the list of effective pages (LEP).

(2) Check that, if any pages have been extracted, they tally with the instructions accompanying the amendment.

(3) Before any extracted pages are destroyed, hand over the documents to an authorised person for checking.

(4) The extracted pages may then be destroyed as required, either in accordance with the amendment instructions, or, as detailed at paras 04034 - 04043.

04020. Personal retention of documents. The personal retention of documents marked SECRET and above at official premises by individuals on a semi-permanent or personal basis is to be discouraged but, where it is unavoidable:

a. A list of documents is to be made, kept up to date, and a copy lodged with the registry. The holding official will sign the list held by the registry to the effect that he/she assumes responsibility for the documents.

b. The documents will be subject to spot checks and regularly reviewed, first for the need to retain them and secondly, for disposal or destruction as appropriate.

c. TOP SECRET documents are to be mustered as required by para 04048 and before the individual relinquishes his/her appointment.

04021. Documents associated with information technology (IT). Information on the marking, recording and storage of documents associated with IT is set out in DMS Vol 3.

Maintenance of files/folders and other covers containing protectively marked documents

04022. Security colour codes. Files, folders and other covers are to be marked to show the protective marking of the contents and should be of the appropriate colour as follows:

a.	TOP SECRET	-	RED
b.	SECRET	-	PINK
c.	CONFIDENTIAL	-	GREEN
d.	UNCLASSIFIED/RESTRICTED	-	BUFF

Production/reproduction of TOP SECRET and SECRET documents

04023. Baseline measure. All originals of TOP SECRET documents must be numbered. If a recipient needs to make copies, his/her original document should be annotated with the number of copies made.

04024. Authorization. Requests for production/reproduction are to be authorized in accordance with para 04005 above. Where work to be done entails the production of printing blocks, eg for diagrams or illustrations, originators must state, at the ordering stage, the protective marking of the diagram, etc, in isolation. Appropriate security measures should then be taken by those responsible for initiating block manufacture.

04025. Typing sections/reprographic pools. The following basic principles are to be observed in typing sections/reprographic pools etc:

a. The receipt and despatch of TOP SECRET and SECRET work is to be recorded. Where work to be done involves a series of processes, progress from stage to stage is also to be recorded. Records are to be checked frequently, causes of delay being investigated to confirm that documents have not been vulnerable to compromise.

b. Supervisors must ensure that all spoiled or rejected copies are destroyed immediately. When not in use, contact material for typewriters, photocopiers, etc (including inked ribbons, paper, negatives, etc), byproducts and pieces of equipment retaining images of documents processed, must be locked away in a container that provides protection commensurate with the protective marking of the information contained therein.

c. Protected waste is to be collected together for removal at least once a day; where this is impossible, collected waste should be locked away by the supervisor in a security container appropriate to its highest protective marking.

04026. Shorthand writers. When requests are made for the services of a shorthand writer, the security grading of the work is to be stated so that appropriate security safeguards may be applied. The following principles are to be observed:

a. Controllers of typists are to issue instructions to typing sections regarding the control of shorthand notebooks used to take down information marked SECRET and above in shorthand.

b. Such information is to be recorded in shorthand notebooks that clearly show the protective marking of the information contained therein and with serially numbered pages.

c. The protection afforded shorthand notebooks must be commensurate with that required for the appropriate level of protective marking.

04027. Audio typing. Audio tapes received by typing sections for the production of protected work should be safeguarded at all times according to the highest protective marking ever recorded on the tape.

04028. Security instructions. Detailed security instructions reflecting the above paras are to be issued to staff by supervisors of typing sections and reprographics installations, etc.

Security of user-held copiers

04029. General. The following paras outline requirements for the control of office machines commonly identified as "photocopiers". Similar safeguards should be applied to other facilities capable of reproducing copies of documents in any form, including viewfoil producing equipment, facsimile terminals, microform equipment, "flipchart" copiers (as used for presentations), computer based image capture devices, etc. (See Chapter 5 Section XV for the detailed physical security measures to be applied to photocopiers.)

04030. Conditions for the installation and use of copying facilities. Where centralised facilities are not available, or are unsuitable, eg for work on specially sensitive or abnormal material, local copying facilities may be provided within Establishments. The following conditions are to be observed:

a. Establishment security officers should always be consulted when considering the introduction of user-held copiers. Such facilities require control to prevent abuse; eg unofficial work or the unauthorized copying of protectively marked documents, and should be supervised at all times. The following requirements should be met:

(1) Photocopiers should only be sited in a supervised environment (ie in an occupied room) or in a separate room to which access is controlled (eg via a simplex lock or swipe card mechanism).

(2) Use of a branch/unit photocopier should be restricted to the members of that branch/unit unless formal arrangements and authorities are organised to provide reassurance that the security controls are not being abused.

(3) Only the copying of documents marked SECRET and above need be recorded in a PDR, supported, if required, by the completion of MOD F 72 or other authorization.

(4) Must be locked at the end of each working day/power supply disconnected and secured.

04031. Where copiers are under the control of supervisors or their deputies, the following procedure must be followed:

a. All staff intending to take copies by operating the machine must ensure that the appropriate authority (MOD F 72 or equivalent) has been raised before SECRET and above documents are copied.

b. Supervisors or their deputies are to carry out spot checks of documents being copied, paying particular attention to protective markings. Any misuse should be investigated immediately. All irregularities should be reported to the Establishment security staff should it appear that protected documents may have been copied without authorization.

04032. Where user-held copiers, and copiers in centralised facilities which are available to other staff, are controlled by automated devices, separate security instructions will need to be promulgated. Advice should be sought from security staff or security units.

Safe custody of material used in the production or reproduction of protected documents

04033. The following document security requirements should be observed:

a. Cylinders, discs, tapes and wires, shorthand notebooks, braille tapes, stencils and carbon papers, etc, used to record protected material are to be safeguarded as protected documents. Carbon paper and stencils, etc, which are not likely to be re-used are to be treated as protected waste.

b. Printer and other inked ribbons and correction tapes (eg acetate, paper, thermal transfer and carbon ribbons) which have been used for protected work must be kept in an appropriate security container when not in use and eventually disposed of as protected waste. All typewriter ribbons, etc, should be removed from equipment before it is allowed to leave official premises for repair.

Destruction

04034. Baseline measure. Documents which are no longer in use and for which there is no longer any adminstrative need, or which are considered unsuitable for consideration for permanent preservation – guidance on the criteria and where to forward relevant material is given in JSP 441 – may be destroyed. Destruction to be undertaken by the originator, successor, or a person duly authorised within the holding department. A record of SECRET and TOP SECRET documents should be made which includes the date of destruction and authorisation.

Disposal of unwanted documents

04035. General. Establishments receiving copies of protectively marked documents in which they have no direct interest should arrange for their disposal in accordance with the following paragraphs. The originator should also be informed so that distribution of further documents can be curtailed.

04036. Documents which holders MUST NOT destroy. Unwanted documents in the following categories must be sent to the authority shown.

Type of document	Action
UK ATOMIC documents, including ATOMIC PRINCIPAL and ATOMIC CONIFER	Return to the ATOMIC Control Officer/ATOMIC Liaison Officer in accordance with ACO 130
US ATOMIC documents	Return to the ATOMIC Control Officer (London) or UKAEA as appropriate in accordance with ACO 130
TOP SECRET IDO accountable documents and all protectively marked ATOMAL documents	Return to the International Documents Registry (DIS Sy IDR)
(1) Cabinet or other ministerial committee papers, minutes of meetings or conclusions (whether protected or unclassified). (2) Extracts from minutes of Cabinet or Cabinet ministerial committees. *Note:* (1) and (2) above do not apply to Cabinet Office official committee documents. These may be destroyed by holders when no longer required.	Return to the Secretary of State's Private Office (Documents held on charge from the Cabinet Office). Return to the Secretary of State's Private Office.
Accountable documents from other Government departments and other documents subject to special control	Return to the publications division or other distributing agency

04037. Documents which holders may destroy. Unwanted documents other than those in categories included above may be destroyed and disposed of as protected waste in accordance with paras 04038 - 04043 below.

04038. Records of destruction. The destruction of documents marked SECRET or above must be recorded in accordance with the following guidelines:

a. The final column of the PDR should be endorsed with the names and signatures of those certifying destruction of individual documents together with the date.

b. Alternatively records may be made using MOD Forms 426 (destruction certificate).

c. Destruction certificates should be kept for 5 years from the date of completion.

d. Destruction of NATO accountable documents, ie those bearing COSMIC and/or ATOMAL markings, should be undertaken only by the International Documents Registry (DIS Sy IDR), who will retain COSMIC destruction certificates for 10 years from the date of completion. ATOMAL destruction certificates are to be retained indefinitely.

e. The destruction of MOD Registered Files is to be certified on MOD Form 262F.

04039. Certification. The destruction of SECRET and TOP SECRET documents is to be witnessed and certified by two suitably vetted persons, one of whom must be an officer not lower in rank than Warrant Officer (or a Senior NCO nominated by the Commanding Officer), Administrative Officer or equivalent. The destruction/certification of documents marked CONFIDENTIAL, where recorded in a MOD F 102, may be undertaken by one authorised member of the Armed Forces or Civil Service.

Downgrading of information

04040. The regular review of holdings of protectively marked documents in any media is desirable in terms of security, cost and convenience. Any review should consider whether the current grading needs to be retained or whether it is possible to downgrade or destroy the material. Only the originator, or successor, may authorize downgrading but exceptionally, where the originator, or successor, cannot be traced, copy documents may be downgraded by the holders after consultation with other addressees. MOD F 171 may be used to request and authorize downgrading. An example is at Appendix 1 to Annex A.

Methods of destruction

04041. General. Protected waste is to be destroyed by machine shredding, pulverising, pulping or burning. Methods which enable protected material to be reduced to unclassified waste before leaving the building/site are preferred. All paper waste is to be destroyed by tearing into a minimum of four pieces and placing in an appropriate Kraft paper sack. Before destruction, magnetic media which has been used to store protected data should be wiped using a security-approved bulk eraser or, where possible, overwritten using an approved erasure programme. If media contains

information protectively marked CONFIDENTIAL or lower it may be disposed of or re-used as though it had never been graded provided an approved erasure package is used. Media which contained material marked SECRET or TOP SECRET may only by re-used if it will continue to attract the same or higher protective marking. If not, it must be destroyed or stored in accordance with approved measures. Detailed instructions are provided in Chapter 5, Section XVI.

Kraft paper sacks for burning/pulping protected waste

04042. In MOD HQ buildings/sites, office keepers are responsible for overseeing the collection, control and safekeeping of sacks or protected waste until destroyed under MOD control or collected for destruction by HMSO. At DPA establishments, messenger services normally undertake these functions. Service Establishments have their own arrangements. Special kraft paper sacks are available from respective staffs for the disposal of protected waste. They are identified by HMSO code numbers as follows:

a. Code 971-003 Multiwall printed in red for burning.

b. Code 971-004 Multiwall printed in black for pulping.

Sacks to be burnt under MOD arrangements are to be securely tied; sacks to be burnt or pulped under HMSO arrangements are to be sealed using a security approved tag or seal such as those issued by the Defence Courier Service.

04043. Messengers, etc, collecting sacks of unshredded waste protectively marked SECRET or above are to keep a permanent notebook record of the following details:

a. Date of collection.

b. Establishment providing waste.

c. Number of sacks collected.

d. Signature of officer handing over waste.

e. Signature of officer receiving waste.

f. Number of sacks sent for destruction.

g. Date sent for destruction.

h. Supervisors signature.

Office keepers, etc, must inspect collection notebooks at intervals to ensure correctness of entries and make spot checks of bags to ensure that quantities in store tally with quantities recorded in the notebooks. Pending destruction, protected waste in sealed sacks is to be kept in secure storage or security containers appropriate to its protective marking.

Spot checks

04044. Baseline measure. Spot checks are intended to ensure that the document control system is adequate and functions correctly and that the rules are being observed by the staff.

04045. Checks. Checks of recorded protectively marked material are an essential part of the system for the physical protection of such material. The detailed requirement for checking is to be included in Establishment Security Standing Orders which must lay down:

a. The material to be checked.

b. The frequency with which the material is to be checked.

c. The appointment of the person responsible for checking.

d. The form of report to be submitted by the checking officer.

e. The action to be taken in the event of losses or discrepancies being discovered.

f. Any special requirements for documents subject to special handling procedures.

04046. Daily checks. There is to be an effective procedure for ensuring that protectively marked material is adequately protected out of working hours. The use of office check sheets (specimen at Annex B) should be considered, and a clear desk policy is recommended.

04047. Protectively marked material left on display. Where there is a requirement to do so, COs/HOEs may authorise the open display of UK RESTRICTED information, for example on notice boards, after taking account of the local security environment and the potential risk and consequences of disclosure to those who potentially have access (eg cleaners/guards). In certain MOD(HQ) buildings, because there will generally be a higher proportion of RESTRICTED information carrying special policy and other sensitivities, material of this level **should not** normally be left on open display. The guidance of local security organisations should be sought as necessary. Material graded UK CONFIDENTIAL and above may only be left on display in secure rooms of the appropriate standard to which only suitably cleared personnel have access.

04048. Checks by security and inspection teams. During all establishment protective security surveys and inspections, security personnel are to make a physical check of all aspects of the security of protectively marked documents. Irregularities in document procedures will be reflected in the resultant report.

04049. Minimum standards for checks and musters. Checks and musters of documents marked SECRET and above are to be carried out to the following minimum standards:

a. **TOP SECRET**

(1) All incoming documents at TOP SECRET protective marking should be page by page mustered on first receipt and before returning the MOD Form 24.

(2) **On Handover of HOE (or equivalent in Headquarters) and TOP SECRET Control Officers (TSCOs).** All TOP SECRET documents are to be mustered and checked against MOD Form 102, or F 6809 where used, the folio sheets of files (MOD F 672) and also checked page by page for presence and completeness; this is to include documents such as bulky publications not held on files. On handover of HOE (or equivalent) this should be done by an officer other than the TSCO or his deputy.

(3) **Annually.** Musters and checks as at (1) above are to be carried out by a person other than the TSCO, Deputy TSCO or person having custody of the documents (unless a muster has been carried out within the last year on handover as at (1) above).

(4) **Monthly.** Spot checks are to be carried out at unannounced random intervals of approximately one month, preferably when work starts or is about to stop, of a number of documents, eg six, selected from both current and open MOD Forms 102 or F 6809; a check that downgrading/weeding action has been carried out is to be included. A specimen Spot Check Report is at Appendix 1 to Annex B.

(5) **Daily.** All TOP SECRET documents in use are to be recalled daily for centralized storage unless retained in accordance with para 04017.

(6) **During security surveys and inspections.** Security survey and inspection teams are to inspect at least 20 documents and 10 files, or the establishment's total holdings, if less than these quantities. Although the majority of the documents and files inspected should be from those originated and received since the date of the last survey or inspection, a small proportion should be selected from before that date. The inspection is to include a check of all TOP SECRET documents which are stored separately (ie not within files).

b. **SECRET**

(1) It is best practise that all incoming documents at SECRET protective marking should be page by page mustered on first receipt and before returning the MOD Form 24.

(2) **Annually**. It is best practice, but not mandatory for all SECRET files to be mustered and checked against file lists; this is to include all SECRET documents not held in files.

(3) **Monthly.** Spot checks as at sub-para a (4).

(4) **During security surveys and inspections.** Inspections of SECRET documents and files as at sub-para a (6).

Note: Additionally, the following TOP SECRET and SECRET documents are also subject to spot checks:

a. Documents including any attachments circulated as loose papers to individual officers (ie without being placed on a file or folder), and which are still on their charge.

b. Documents which are being typed or reproduced.

c. Shorthand notebooks.

d. Film, transparencies, slides, viewfoils, etc (checks including physical examination and comparison of content with listed holdings to guard against substitution).

c. **CONFIDENTIAL**. It is best practice, but not mandatory, for CONFIDENTIAL files, bearing caveats for which access is controlled by induction or indoctrination and therefore require the contents to be accounted for in a MOD Form 102, to be mustered annually against the master file list. Such material, together with items not held in files, eg Books, Equipment and Magnetic Media, are to be subject to Spot Checks.

04050. Records of checks and musters.

a. Records of checks and musters are to be kept by establishments for 2 years. These records are to show:

(1) The type of check or muster, with dates, carried out.

(2) The files and documents seen and by whom.

(3) Details of any irregularities found and action taken to rectify them.

b. Completion by Army units of the checks and musters at paras 04044 - 04049 is to be confirmed as part of the annual report on a unit (see AGAl paras 2091 to 2100).

04051. Microform. In order that the spot checking officer can verify that a jacketed fiche master copy is complete, a diazo copy, which cannot be tampered with, should be made for comparison purposes and should be replaced with a fresh copy whenever the master is amended. The silver halide master and the diazo copy must he stored separately. In addition, the following points affecting the integrity of microfilm should be noted:

a. **Aperture cards.** As well as checking the microform against the register, it is desirable to check periodically that the correct image is in the card.

b. **Roll film**. Check the container details against the register and periodically put the film on a reader to ensure that it is the correct film, that frame numbers are in sequence and the diazo film is free from splices.

c. **Jackets.** Check periodically the contents of the film in the Jacket against the diazo duplicate to detect possible substitution of the film strip in the jacket.

d. **Microfiche.** Check periodically that all fiche in sets are present and that no improper substitution has been made.

04052. The officer conducting a spot check is to report to the head of establishment or the nominated security officer. The report must contain the details as shown at Appendix 1 to Annex B.

04053. HOE should ensure that all irregularities noted in reports are resolved. Significant irregularities or any which cannot be resolved locally are to be reported to the appropriate Principal Security Adviser's staff who will notify DDefSy where appropriate.

04054. Reports are to be retained personally by the head of establishment or the nominated security officer and, to ensure that spot checks are completely random, are not to be made available to spot checking officers or to other members of the staff. The reports are to be made available to security inspectors during security surveys/inspections, investigations or advisory visits.

Musters

04055. TOP SECRET files are to be mustered annually. Musters ensure that TOP SECRET files are not lost between the registry and areas served, a fact which would not be disclosed by the system of spot checks outlined above. Special rules exist for mustering ATOMIC and certain other documents on limited distribution. These are in no way invalidated by the procedures outlined above. Certain documents originated by

other Government departments and used within the Ministry of Defence may also be subject to mustering and accounting procedures. Accountable IDO documents will be mustered once every twelve months under arrangements made by DIS Sy (IDR).

SECTION II

TRANSMISSION OF PROTECTED DOCUMENTS

Baseline measures

04056. Protective markings of SECRET, CONFIDENTIAL and RESTRICTED assets should not appear on the outer cover, packaging or container sent outside an establishment. The protection given to assets sent to or received from other countries must take into account any international agreements on the carriage of protectively marked assets. For TOP SECRET see Appendix 1 to Annex C.

General

04057. Protectively marked documents are to be prepared for transmission in accordance with the instructions contained in Annex C and its Appendices;

a. The instructions contained in this Chapter relate to protectively marked documents which do not bear supplementary restrictive markings (other than the simple prefixes "UK" denoting documents of UK origin and "NATO" or "WEU" identifying International Defence Organisation [IDO] documents).

b. Procedures governing the transmission of documents bearing markings such as "ATOMIC" and "ATOMAL", etc, and documents subject to special handling arrangements, are issued separately to those with 'need to know'.

c. Persons receiving documents bearing markings which are unfamiliar to them should consult their establishment security officer (ESyO).

Note: Care must be taken when addressing letters, etc, and their envelopes/packaging, to ensure that details entered are clear, complete and correct; similarly include an address to which replies can be sent. Detailed instructions for preparing envelopes/packages containing protected material will be found at Annex C to this Chapter. Certain material must be addressed to the recipient by name. Mail for organisations listed in the MOD Directory should be addressed to branches, etc, identified by abbreviated titles.

04058. Officers receiving protected or sensitive documents which are not of their concern, are responsible for the items' onward despatch to the proper addressee or return to the originator. Appropriate safeguards, as laid down in this Chapter, must be applied. Where the consignor appears to be in breach of security regulations, the establishment security officer should be informed who will take reporting action as necessary.

Files

04059. When files bearing different protective markings are transmitted together, the file bearing the highest marking is to be placed topmost inside the envelope or wrapping. Files are to be securely fastened together and prepared for transmission in accordance with instructions appropriate for the highest protective marking.

Packaging

04060. To reduce risk of loss or compromise during transmission, particular care is to be taken when packing protectively marked documents or material. For detailed advice on the correct way to package bulky/awkwardly shaped items, staff should contact their local mail room or consult JSP 367. However, the following points are to be considered:

a. Selection of the correct envelopes/packaging commensurate with the weight and size of items for despatch is vital.

b. Corners of stiff-covered documents can easily tear through envelopes or other wrappings. To prevent compromise due to torn packaging, staff should consider the use of “Jiffy” envelopes and “bubble wrap”.

c. Extra strength can be provided by applying cellulose or adhesive tape or by double wrapping (even though the latter may not be called for on security grounds*).

d. Extra care must be taken when packing documents, etc, as parcels (even when sent by "Letter Post") will be subject to rough handling during sorting and transmission.

e. If necessary, extra-strong envelopes are available to special order through CS(PS). Linen sacks may also be used for bulky consignments.

*Where applicable (see Annex C), double cover must be provided irrespective of the type of packing or method of transmission.

Methods of transmission

04061. Certain documents, identified by their protective marking and/or destination (see Annex C) must **never** be sent by Post Office services;

a. It is mandatory for TOP SECRET and cryptographic material to be transmitted by hand to hand with the provision of auditable receipts at each transfer.

b. External services (other than the Post Office) may only be used for transmission of material marked CONFIDENTIAL or SECRET where approved by DDefSy.

Approved methods of transmission

04062. A number of mail services operate within/between MOD establishments and the Services. The British Forces Post Office carries mail between establishments/buildings in London and the Home Counties. (Details of locations served are published in JSP 367; see also Annex C, para 3). Other services operate between neighbouring establishments/sites under local arrangements. Annex D provides summary details of transmission.

Restrictions on display of national caveats on envelopes

04063. National caveats must not be visible on any envelope in transit. Detailed instructions regarding the protection and transmission of such material are issued separately on a 'need to know' basis. The occasions when standard protective markings should be shown on envelopes are identified in Annex C and must be followed.

Use of window, transit and self sealing envelopes

04064. Window, transit and self-sealing envelopes must not be used for the transmission of documents marked RESTRICTED or above.

Sealing - general

04065. All envelopes, packages and sacks, etc, containing TOP SECRET material, and similar consignments of SECRET material for delivery abroad or in Northern Ireland, are to be sealed to guard against surreptitious tampering. The following paragraphs describe alternative methods to be employed.

High security tape

04066. Red high security tape is no longer supplied by the Stationery Office. However existing stocks should continue to be used to exhaustion. It should be applied to envelopes containing material marked TOP SECRET, and to **inner** envelopes containing SECRET material intended for despatch to addresses abroad or in Northern Ireland. (Annex C, Appendix 1 and Section IV of Appendix 2 refers). Application of the tape is detailed in Appendix 5 to Annex C.

04067. High security tape is **not** suitable for use other than on envelopes; conventional wafer seals are to be applied to parcels and packages and metal seals to mail sacks, etc (see para 04077).

04068. Storage, maintenance and disposal of high security tape. The following should be observed:

a. The tape should remain sealed in the polyethylene wrapping in which it is supplied until required for use.

b. To avoid deterioration, high security tape should be stored away from direct sunlight and sources of heat, in a frost free environment without extremes of humidity or temperature (ie 30-60% relative humidity and 15-25 degrees centigrade) and should not be exposed to adverse conditions for extended periods.

c. High security tape has a shelf-life of twelve months when stored under recommended conditions. Rolls of tape will be serially numbered during manufacture to facilitate sequential use and allow identification should this be necessary.

d. Rolls, lengths and waste portions of high security tape, including any remaining on used envelopes, should be protected to RESTRICTED standards and kept under lock and key. Waste tape and used envelopes bearing high security tape **should be treated as protected waste** and disposed of in accordance with the relevant security regulations.

04068. Evidence of tampering. While use of high security tape on envelopes will deter surreptitious attack, staff should be alert to the possibility of tampering. Those receiving envelopes to which tape has been applied should look for the following:

a. Colour run of tape.

b. Damage to serrated edge of tape.

c. Blurring of the tape underprinting.

d. Evidence of underprinting remaining as green or blue image on envelope surface indicating the tape may have been repositioned.

e. Evidence of slitting along flap or seam (indicated when flexing the envelope along its flap/seams shows the colour of the envelope through the tape).

Where tampering is suspected, establishment security officers should be alerted. When opening the envelope, care must be taken to ensure that evidence is not disturbed. Reports of possible tampering should be forwarded through establishment security officers to security units together with the envelope.

04069. Alternatives to high security tape. Until a suitable, economically acceptable alternative to the high security tape can be found, staff should select from the tape and seals detailed below which are suitable for sealing envelopes, packages, parcels and boxes and have been approved by SEAP. Your Principal Security Adviser's staff may be able to provide further advice, if required.

Product	Security Class	Company
Applied Holographics tamper-evident surface seals	Low/Medium	Applied Holographics (Tel: 0191 4175434)
MARKITWISE surface seals (especially types: GR/2, MRP/2, S & Micro LA)	Medium/High	Markitwise International (Tel: 01886 812427)
GOSHERON tamper-evident tape (polyester & polystyrene)	Medium	John Gosheron & Co Ltd (Tel: 0181 847 3901)
GOSHERON surface seals (types: D201-A, D210-V, C222 & V223)	Low	John Gosheron & Co Ltd (Tel: 0181 847 3901)

Notes:

1. The level of security offered by these alternatives is less than was available from the red high security tape.

2. The Keepsafe envelope is still available and offers the security and a high level of integrity for the transmission of SECRET and TOP SECRET material.

Keepsafe security envelopes

04070. Keepsafe security envelopes are approved for the transmission of TOP SECRET, SECRET and material requiring controlled distribution abroad, and of TOP SECRET material transmitted within the UK and Northern Ireland.

04071. The approved Keepsafe security envelopes are available in a range of sizes, are opaque and made from super strength plastic film. They incorporate a specialised closure system offering maximum evidence of tampering and other security features as follows:

a. Each envelope is printed with a unique identification number located on the envelope, and on the closure and label flaps.

b. The label flap has been added to enable addressees to affix labels to it when required because, for security reasons, labels must not be fixed to the main body of the envelope.

c. The secure portion of the envelope is surrounded by a printed "chain", designed to provide evidence of tampering.

04072. Consignees should bear in mind that when sending material in Keepsafe security envelopes for onward transmission via a forwarding agent (eg the Defence Courier Service (DCS)) protective or other markings may be masked by overwrapping. Arrangements should therefore be made with such organisations to ensure that the material receives appropriate handling through all stages of its journey.

04073. Addressing and sealing. The following procedure should be followed when addressing and sealing Keepsafe security envelopes:

a. When the receipt for the material to be transmitted is prepared, the unique serial number of the Keepsafe envelope should be included on the receipt.

b. The main body of the Keepsafe envelope is marked and addressed in the same way as an envelope to be sealed with high security tape **(Note: use ball point pen - do not use labels or stamps).**

c. Adhesive address labels must only be affixed to the special flap provided for such labels/stickers or stamps. When using such items, the envelope number on the flap must not be obscured.

d. The material to be transmitted is placed in the Keepsafe envelope.

e. The Keepsafe envelope is then sealed as follows:

(1) On a flat surface remove the printer release tape from the special adhesive strip.

(2) Allow the closure flap to fall naturally over the envelope mouth, and then press down on the adhesive strip so that the number of the envelope remains legible. The envelope is correctly sealed only when the printed release tape has been removed. Envelopes must not be patched until they have been correctly sealed. Special attention should be paid to sealing when the item to be transmitted is not flat; sharp edges or points should be masked.

f. Where it is required that the Keepsafe envelope should be covered, it must be placed inside another **opaque** cover, addressed and sealed as appropriate (the cover need not be another Keepsafe envelope).

04074. Evidence of tampering. While the Keepsafe envelope will deter surreptitious attack, staff should be alert to the possibility of tampering. The following procedure for establishing whether an envelope has been tampered with may seem extensive, but evidence of tampering can be spotted at a glance when the process becomes familiar:

a. Ensure the envelope's high security closure has been sealed.

b. Examine the envelope's surfaces, which should be white, unbruised and with no visible cuts.

c. Examine the four sections of "chain" printing surrounding the secure portion of the envelope; they should be straight, continuous and with complete chain printing on the front of the envelope.

d. Ensure the number on the keepsafe envelope corresponds with that on the closure and label flap.

e. Examine the specialised closure system:

(1) There should be no blurring, distortion or disruption of any of the black lettering, numbers or sharp patterns.

(2) The envelope is designed to have a narrow black strip at either end of the closure strip.

(3) The red colour should be continuous; no change in colour should be present; look especially for black, white or yellow staining.

(4) The closure must not have any added reinforcing (eg cellulose tape).

Where tampering is suspected, establishment security officers are to be alerted. Advice on the enquiries required by the establishment security officer may be obtained from security staffs.

04075. Storage. Keepsafe envelopes:

a. Should be stored in cool, dark conditions, and in their original packaging until used.

b. They should not be stored in excess heat or cold.

c. It is important that they are not exposed to sources of ultraviolet radiation, such as strong sunlight or positioned close to fluorescent lamps.

d. Under these conditions, the envelopes should have a shelf-life of at least 12 months.

e. The envelopes should be kept in lockable containers to prevent unauthorized access.

f. Once used, those Keepsafe envelopes bearing markings which themselves are protected (eg CODEWORDS) should be treated as protected waste and disposed of in accordance with the relevant security regulations.

04076. Procurement. Keepsafe security envelopes are available from two sources:

a. HMSO, Bristol through normal channels. Contact point is as follows: HMSO, Bristol Distribution Park, Hawkley Drive, Woodlands Lane, Bradley Stoke, Bristol BS12 0BF. Customer enquiries: 01454 621 200. They are supplied as follows:

HMSO Product Code	Dimensions	Quantity per box
027-4000	460x377mm + label flap(A3 Wide)	250
027-4001	330x462mm + label flap(A3 Long)	250
027-4002	280x385mm + label flap(A4)	500
027-4003	195x285mm + label flap(A5)	250

b. Trigon Cambridge Ltd. Contact point is as follows: Customer Service Department, Trigon Cambridge Ltd, Saxon Way, Melbourn, Royston, Herts SG8 6DN. Telephone 01763 261 900. They are supplied as follows:

STOCK Code	Dimensions
HRDC A3W	460x377mm + label flap(A3)
HRDC A3L	330x462mm + label flap(A3)
HRDC A4E	280x835mm + label flap(A4)
HRDC A5E	195x285mm + label flap(A5)

Approved security seals and ties

04077. Where the item to be sealed is not contained in an envelope, *security* approved seals are to be used. Parcels and packages should have wafer seals applied along all seams at intervals not greater than 100mm. If the item is bulky it should be inserted in an appropriate sized mailbag (these can be supplied by the local mail room) and tied with an approved tie and sealed.

a. **Wafer seals** are to bear a recognisable signature in ink, the signature being part on the seal and part on the wrapping; all seams and seals should be fully covered with strips of transparent cellulose tape.

b. **Bags and seals.** Mail bags or sacks used for the transmission of bulky protectively marked items should be robust and not have any holes or patches on them. They should be tightly tied and sealed using approved security seals such as those provided by the DCS or supplied in the Catalogue of Security Equipment.

Where an address label, ie self-addressed label or MOD Form 488, is used with wafer seals, the label should be stuck down first before applying any seals.

Receipting

04078. Receipts are to be obtained confirming delivery of the following:

a. TOP SECRET documents and material.

b. SECRET documents transmitted outside a building/site (see Appendix 2 to Annex C).

c. Other documents where transmission is subject to special handling instructions issued on a 'need to know' basis or where the originator requires confirmation of delivery.

In addition to receipts completed by the addressee, MOD Forms 32 (providing a record of hand-to-hand transmission with date/time of despatch/receipt) are to be used when envelopes, packages, boxes, etc, containing TOP SECRET material are carried between establishments.

04079. Receipts rendered in accordance with para 04078 above may be standard MOD Forms 24 or specially prepared proformae, eg produced as a tear-off strip on a distribution sheet. In either case, the receipt should identify the following:

a. The consignor's address - to which the receipt is to be returned.

b. Details of the document transmitted - typically reference number and date plus copy number (if any); the document title should **not** be shown.

c. Details confirming receipt of the subject document - the signature, name (in block letters) and official address (branch stamp, etc) of the individual opening the envelope or package.

04080. Receipts are to be completed and returned to the consignor immediately following delivery of the subject envelope, etc. They should normally be completed by registry staff immediately prior to making PDR entries. Where envelopes, etc, are addressed "Exclusive to..." and delivered to individual officers, those officers should

complete any receipt enclosed before arranging for PDR entries to be made. See also sub para 04013(c).

04081. HOE are responsible for ensuring that receipts against items despatched from their areas are returned promptly - within the time normally taken for transmission over the route concerned (eg 10 working days for transmission within the United Kingdom). Failure to respond quickly can result in detection of loss and compromise of sensitive material being seriously delayed. Consignors who identify addressees who persistently fail to return receipts promptly should report the matter to the establishment security officer.

04082. Completed receipts, other than those relating to accountable documents (see Definitions) for which separate instructions apply, are to be retained for two years.

Opening and examination of envelopes, packages, bags, etc

04083. A local record is to be maintained of officers authorized by HOE to open TOP SECRET envelopes, etc.

04084. If the person opening an envelope or package containing material marked SECRET or above suspects that it has been tampered with, the head of establishment, via his security representative, should be informed. The latter should consult the respective security staffs as necessary. The documents concerned and related envelopes, etc, should be set aside and handled by the minimum number of other persons in case forensic examination is required.

04085. Before envelopes, mailbags and other containers used in the transmission of protectively marked or sensitive material are discarded, they should be carefully checked to ensure that they are empty.

04086. No unopened mail is to be left out on display in empty offices or registries. All unopened mail is to be locked away in an approved combination lock security container.

Boxes, pouches, etc

04087. A locked box or pouch is acceptable as outer cover to an envelope or package containing a protectively marked document which would otherwise be transmitted 'double enveloped' (see Annex C). They should normally be used for transmission between a central controlling organisation, eg a registry, and another permanent address, keys being held by both.

04088. Boxes, etc should be addressed to a key-holder, by appointment or name and appointment. Where delivery of a box, etc, containing protectively marked material to a minister, etc, is not practicable using normal methods of transmission (eg MOD van service, car or courier), the appropriate Principal Security Adviser's staff should be consulted.

04089. Where boxes, etc, are used to transmit a number of documents to a distribution point, eg a mail room, consignors must place documents in envelopes addressed to individual recipients so that 'need to know' is maintained after the box, etc, has been opened.

04090. Empty containers are to be returned to the controlling organisation without delay. Boxes, etc must not be used by recipients to send protectively marked documents, etc, to addressees other than the controlling organisation. Controlling organisations are to record the movement of their boxes, etc, and investigate where any are not returned within six working days.

04091. The security of a suite of boxes, etc, may be compromised by loss of a key or when an unauthorized person has the opportunity to examine the lock. When not in use, they are to be kept locked and stored under lock and key. When delayed in transit, boxes, etc, are to be stored in a security container.

04092. When not in use, keys to boxes, etc, should be kept in a locked security container. Boxes, etc, and their keys are to be mustered twice a year by the controlling organiser. Key holders are personally responsible for the safety of keys in their charge. Before handing-over official responsibilities, including handover to cover temporary absence, keys are to be formally mustered and transferred to another officer. Any changes in holders of boxes, keys, etc, are to be reported to the controlling organisation immediately.

Despatch of protectively marked documents to private addresses in Great Britain

04093. Documents marked CONFIDENTIAL or above are not normally to be sent to private addresses. When this is unavoidable, or where officials or consultants are authorized to work at home, the following rules are to be observed:

a. TOP SECRET documents are not to be sent without specific approval by PUS. Where approved, documents must be conveyed by hand of an authorized courier.

b. TOP SECRET, SECRET or CONFIDENTIAL documents are not to be sent to addresses where:

(1) A foreign domestic servant is known to be employed; or

(2) Where there is no container of appropriate standard in which to keep them.

c. The consignor is to contact the addressee and obtain confirmation that:

(1) The provisions in sub-para 'b' are satisfied; and

(2) The addressee will be on hand to receive the documents.

d. Subject to the conditions at sub-paras 'a' to 'c' above, protectively marked documents should be despatched in accordance with the procedures at Annex C. If the addressee is likely to be away from the address to which protectively marked documents are about to be sent, they must not be despatched.

Note **:** Where TOP SECRET or other documents are to be sent by courier, the addressee must be warned that he/she must receive them in person, producing identification to the courier's satisfaction before the documents can be handed over.

04094. If the intended recipient has no security container of appropriate standard in which to store documents, they are to be despatched to the security officer of the nearest MOD/Navy/Army/Air Force establishment. The consignor is to:

a. Instruct the establishment to hold the documents in a sealed envelope for the intended recipient to see (but **not** to remove from the establishment or retain); and

b. To inform the intended recipient where the documents may be seen.

The intended recipient is also to be informed that, after examination, the documents must be replaced and resealed in an envelope for return to the consignor via the holding HQ/Unit or, if needed for future reference, for retention by the latter.

Despatch of other mail to private addresses in Great Britain

04095. Where RESTRICTED or UNCLASSIFIED correspondence has to be sent to a private address, care must be taken to ensure that no wording or marking can connect the addressee with the department. In the case of correspondence to be sent to ex-Service personnel, the use of their former Service ranks and decorations is to be avoided unless they specifically instruct otherwise.

Addressing of mail to private addresses (including civilian firms) in Northern Ireland and the Republic of Ireland

04096. The personal security of Service personnel, civilians and their families and ex-Service personnel resident in Northern Ireland and the Republic of Ireland can be compromised by incorrect transmission of official mail to private addresses (including civilian firms). Material marked CONFIDENTIAL or above must **never** be sent to a private address in Northern Ireland or the Republic of Ireland. The following rules must be observed when transmitting (including redirecting) RESTRICTED or UNCLASSIFIED mail:

a. RESTRICTED and UNCLASSIFIED mail is normally to be addressed via a Service establishment identified by BFPO number (except for mail to the British Embassy in Dublin – see sub-para 04096b below.).

b. Where, in exceptional circumstances, correspondence has to be sent to a private address (as is the case for all such mail to the British Embassy in Dublin) the following rules must be observed:

(1) Use a plain envelope or wrapping without pre-printed official markings such as "On Her Majesty's Service" or MOD Form numbers.

(2) Address carefully and correctly, including the post code, ensuring no reference to rank, decorations or appointment is shown on the envelope.

(3) Do not stamp the envelope with any official stamp or add any detail which could associate the item with the Ministry of Defence.

(4) Postage stamps **must be used in all cases**, do not use franking machines or PPI impressions, labels or stickers.

(5) No return address is to be shown on the envelope that indicates that the sender is associated with the MOD or Services. PO Box 701 is **not** to be used as a return address.

(6) Parcels to the Republic of Ireland must have a customs pack affixed - Post Office Form PFU 5 (**not** a Service type customs form).

Transmission of mail to addresses overseas via diplomatic bag

04097. All TOP SECRET, SECRET and CONFIDENTIAL mail for despatch to addresses outside the United Kingdom must be sent by diplomatic bag or an approved courier service. Despatch procedures, described in Annex C, should be read in conjunction with the following guidance.

04098. RESTRICTED and UNCLASSIFIED mail (other than unclassified publicity and information material) addressed to British Embassies or consulates in countries presenting a special security risk (see para 6 of Annex C) must be sent by diplomatic bag. RESTRICTED and UNCLASSIFIED mail for other overseas addresses may be sent through normal postal services, including (for BFPO numbered addresses) the British Forces Postal Service.

04099. The envelopes/wrappings of all mail to be sent by diplomatic bag (including UNCLASSIFIED which **must** be so marked) are to be marked "Certified Official" and endorsed by a service officer or civilian of at least executive officer grade or equivalent. However COs/HOEs may in exceptional circumstances nominate suitable SNCOs or AOs to complete the task. In addition:

a. The protective marking (or UNCLASSIFIED) should be stamped boldly in red above and below the address.

b. The despatching organisation and the reference and date of origin of the document enclosed should also be shown.

c. Envelopes/packages prepared in this way are then to be sent in a second envelope to HQ DCS, BFPO 747 or LCT, BFPO 1000 in accordance with Annex C.

04100. Private mail for Service personnel and Defence Attaches serving in diplomatic posts in countries of special security interest (see para 6 of Annex C) should be sent c/o Private Letter Section, F&CO, via HQ DCS, BFPO 747.

Transmission of mail to British Forces Post Office (BFPO) addresses

04101. Mail for diplomatic and Service posts, including HM Ships and international organisations should include a BFPO number in the address, where one is in use. Details of BFPO addresses are published in JSP 367.

Transmission of mail to foreign governments and foreign-based defence contractors

04102. Documents marked SECRET, CONFIDENTIAL and RESTRICTED for despatch to foreign governments or foreign-based defence contractors must be prepared in accordance with procedures detailed at Annex C.

04103. The 'despatching authority' must ensure that the originator has approved release of their UK marked information to the recipient country. Where there is any doubt, the appropriate Principal Security Adviser should also be consulted. Where the intended recipient is a foreign-based defence contractor, the despatching authority must also consult InfoSy(Industry)1 to ensure that the recipient company is authorized to safeguard and store protectively marked material at the appropriate level.

04104. Mail received from UK defence contractors for onward transmission overseas is only to be released in accordance with the rules contained in Chapter 11.

Despatch of protectively marked documents to UK defence contractors

04105. Documents marked CONFIDENTIAL or above which are to be sent to List X companies must be addressed via the site security officer - identified by name only; the words "security officer" **must not** be shown on the envelope or wrappings. Mail for companies which have only received provisional clearance should be addressed to the recognised contact who must ensure that the material is properly recorded and safeguarded.

Note: Names of security officers in List X companies may be obtained from InfoSy(Industry) 2/3.

Transmission of mail to private addresses overseas

04106. No protectively marked mail is to be despatched to any private address overseas without prior reference to security staffs.

Transmission of mail to HM Ships

04107. TOP SECRET, SECRET and CONFIDENTIAL mail for HM Ships, RFAs or other authorities afloat in home waters or abroad must be prepared for transmission in accordance with the procedures at Annex C. In addition:

a. Outer envelopes/wrappings should be marked "HMS..., c/o BFPO 999" to ensure correct handling within UK and prevent protectively marked mail passing through foreign postal channels in the event of sudden departure or diversion of the ship.

b. RESTRICTED mail should also be despatched in accordance with Annex C. Envelopes/wrappings should, however, be addressed to "HMS..., BFPO..." (insert number of ship as issued in JSP 367).

Transmission of cabinet and ministerial committee documents

04108. Procedures governing the transmission of cabinet and ministerial committee documents are laid down in "Getting it Done" The Ministry of Defence Office Guide (MOD Manual 2).

SECTION III

REMOVAL OF PROTECTED MATERIAL FROM OFFICIAL PREMISES

Introduction

04109. The removal of protectively marked material from official premises exposes it, and often the carrier, to additional security risks. Protectively marked documents are not to be taken away from official premises unless this is absolutely unavoidable and essential for the conduct of official business. Every effort should be made to reduce the risks associated with hand carriage by sending material through official channels (including use of the DCS), and restricting documents carried both to the minimum quantity and the lowest protective marking. Removal is subject to conditions laid down in the following paragraphs. References to "protectively marked documents" relate to documents marked CONFIDENTIAL or above.

04110. Documents marked SECRET or above are only to be taken outside official premises by individuals holding written authority to do so (MOD F 924 or locally produced alternative). A specimen is at Appendix 2 to Annex A.

a. **TOP SECRET and ATOMIC documents.** Written authority to remove documents marked TOP SECRET or ATOMIC can only be given by HOE or Capt RN, Col, Gp Capt, Grade 7 or equivalent status or, where appropriate delegated authority has been given, by independent unit commanders. Authority should only be given in exceptional circumstances. (See ACO 130, Chapter 4, for correct procedures regarding ATOMIC documents).

b. **SECRET documents.** Written permission is to be obtained from the HOE. Authority to sign MOD forms 924 may be delegated to senior members of staff (not normally below the rank of Lt Cdr, Maj, Sqn Ldr, HEO or equivalent) at the discretion of the head of establishment.

HOE are to satisfy themselves that the security risks involved in removing protected documents from official premises are justified in the public interest. Before departure, officers authorized to remove protected documents are to be briefed on their safe custody during transit and, if appropriate, overnight. Documents remain the responsibility of the named individual until returned to the holding establishment or handed-over to another authorized person (or official representative, eg contractor).

(***Note:*** Briefcases, etc, are not approved security containers and cannot protect contents against surreptitious examination by unauthorized persons (even if given only limited access). Briefcases and other containers used to transport protectively

marked/sensitive material must remain under the carrier's personal custody at all times until their contents can be secured in accordance with minimum security standards.)

Removal for return or delivery within the same working day

04111. Protected documents may be removed from official premises where they are required for reference, etc, at a meeting subject to the following:

a. Files/folders should be checked for completeness before removal.

b. Documents should be carried in a locked container (either a sturdy dual combination lock commercial type briefcase or officially approved box, bag, case or pouch).

c. Documents removed by persons acting as couriers for delivery to third parties should be prepared and packaged as detailed in Section II.

d. The signed (top copy) of MOD Form 924 (or alternative) is to be carried by the officer authorized to remove documents and presented on demand to any person empowered to search briefcases, etc, - eg a security guard. The duplicate form is to be retained by an officer appointed by the head of establishment in accordance with local security instructions.

e. On return to the office, all documents removed are to be checked against the duplicate MOD Form 924 by another officer. Files/folders should be examined to ensure that they are complete. The duplicate form should then be endorsed by the checking officer to confirm safe-return of each item listed. Discrepancies are to be investigated immediately as potential breaches of security.

Removal for retention outside official premises for one or more nights

04112. Protectively marked documents should only be retained outside official premises if they cannot be returned to the holding office, or alternative official premises.

04113. Permission, as a "standing authority" or for a single occasion, may be granted subject to the following conditions:

a. **Standing authority (for overnight working at home).** Where a regular and long-term need can be established for an officer to take protectively marked documents home, the officer must be provided with a security container suitable for their storage, the container being installed under arrangements made through the appropriate Principal Security Adviser (for homeworking rules see Annex M).

b. **Single occasions (for retaining documents overnight at home or in an hotel,etc).** An officer authorized to remove documents is responsible for ensuring that they are safeguarded, remaining in his care **at all times** (see para 04115 below).

Authorization - review of MOD forms 924

04114. HOEs are to establish procedures for periodic review of MOD Forms 924 to ensure that authorizations are not being given without proper consideration. Duplicate copies of the forms should be retained for 2 years and made available for inspection by the appropriate Principal Security Adviser's staff.

Carriage of official documents by officials travelling within Great Britain or Northern Ireland

04115. When authority has been given for documents marked CONFIDENTIAL and above to be taken out of official premises for intended use elsewhere in Great Britain or Northern Ireland, they are to be carried in a locked container (see para 04111) and remain in the care of the authorized officer at all times until they are housed under officially approved arrangements. Each container is to bear a label securely attached to the outside (with a similar label affixed inside) giving instructions to a finder. Only one side of the label should normally be visible, the reverse being obscured by a protective cover. The visible side of the label is to read:

"IF FOUND PLEASE SEE INSTRUCTIONS ON THE REVERSE SIDE OF THIS LABEL".

The reverse side is to read:

"ANYONE FINDING THIS CONTAINER IS ASKED TO TELEPHONE …….. OR HAND IT IN AT THE NEAREST POLICE STATION OR RAILWAY OR OTHER TRANSPORT AUTHORITY WITH A REQUEST THAT THEY SHOULD TAKE THAT ACTION."

(The telephone number to be given is that of the security control room for your building/establishment. If in doubt, consult your Principal Security Adviser for advice.)

While carrying protectively marked documents, briefcase, etc, keys should be kept secure on the person, separate from the container.

Note: Authorised officers must not carry the prohibited items listed at Annex N para 2 in their briefcase with protectively marked documents.

04116. Officials travelling to Northern Ireland should carry documents in a sturdy dual combination locked commercial type briefcase, **not** one bearing the Royal Cypher.

04117. Any briefcase may be used when carrying material marked RESTRICTED provided it is locked (but see para 04116 regarding advice on travel to Northern Ireland).

04118. Protectively marked documents are not to be consulted or worked on anywhere where their contents might be overlooked or otherwise noted. Documents protectively marked CONFIDENTIAL and above are not to be left unattended in any place, such as an hotel, restaurant, taxi, public service vehicle or railway carriage. They are not to be entrusted to the custody of a member of the public (eg by being placed in an hotel safe), or left locked in an unattended motor vehicle. However, documents protectively marked up to RESTRICTED may be left unattended in a locked hotel room or in a locked boot of a motor vehicle provided they are contained within a sturdy dual combination locked commercial type briefcase.

04119. Wherever possible (and particularly where long journeys and overnight stops are likely):

a. Protectively marked documents are to be sent ahead by secure means and addressed for the official to collect on arrival.

b. Arrangements are to be made by the convenor of the conference or meeting, etc, to safeguard protectively marked documents belonging to visitors who have to stay overnight away from their own office.

04120. Where these arrangements are not practical, the following conditions apply:

a. **Retention at home (ie normal place of residence).** Documents marked CONFIDENTIAL or above must not be left in an unoccupied house or flat, etc; they must not be left in the care of other residents. RESTRICTED documents are not to be left unattended unless locked inside a container **to which only the officer has access.**

b. **Retention in an hotel room, etc.** Documents marked CONFIDENTIAL or above must not be left unattended nor entrusted to the care of persons other than Government officials or representatives. RESTRICTED documents contained within a sturdy dual combination locked commercial type briefcase may be left unattended in your locked hotel room.

04121. Travel involving private/official vehicles. Protectively marked material must not be left in an unsupervised vehicle.

04122. Travel by civil aircraft within UK. When travelling by civil aircraft within UK (including Northern Ireland), staff may be required (as a precaution against possible terrorist action) to assist airport security staff, by disclosing the contents of their hand luggage, including briefcases. To prevent compromise of material protectively marked SECRET or above, the following procedures are to be followed:

a. **Prior to departure.**

(1) Complete MOD form 924.

(2) Place the document(s) to be removed from official premises in an unused envelope and stick down the flap.

(3) Courier's name and destination is written on the front of the envelope, adding the branch stamp and reference number of the document(s) enclosed at the bottom left hand corner.

(4) Lock the package and top copy of the MOD form 924 in a sturdy dual combination lock and labelled commercial type briefcase; the package should normally remain inside the briefcase until it reaches its destination.

(5) Airport security may require sealed packages to be electronically scanned before loading as hand luggage. If there is any risk of the contents being damaged by scanning, couriers should seek advice from the appropriate Principal Security Adviser prior to departure.

b. **If challenged by airport security staff.**

(1) If asked by airport security staff to open the briefcase, the MOD officer should explain, discreetly, that it contains official documents carried in pursuit of HMG business; to avoid public recognition as a MOD official and to avoid the material carried being compromised, the courier may ask for any search to be conducted in private. The briefcase may be opened and the MOD Form 924 offered as confirmation.

(2) The sealed package should not be opened except in the presence of senior security staff and then only sufficient to display the nature of the contents, eg papers; uncleared persons must not be allowed to read or otherwise study sensitive material.

(3) Airport security staff should be asked to assist the officer, as necessary, in resealing any package opened at their insistence.

c. **Return journeys.** Similar arrangements are to be made where material has to be returned by hand. Officers carrying protectively marked material should inform the appropriate Principal Security Adviser's staff, through their local security officer, of any difficulties encountered when following the procedures outlined above.

Note: The advice contained in this paragraph applies also to ferry journeys between Great Britain mainland and Northern Ireland, where similar checks may be made at departure points.

Carriage of official documents by officials travelling overseas

04123. Normally, documents marked CONFIDENTIAL or above required by an official after arrival overseas should be dispatched in advance, allowing adequate time for their arrival. The DCS is responsible for the movement of all MOD material marked CONFIDENTIAL and above overseas. This service must be used except in very exceptional cases which require clearance from the appropriate Principal Security Adviser. Exceptional circumstances **DO NOT** extend to TOP SECRET material. Under no circumstances may IDO accountable documents, eg those bearing COSMIC and/or ATOMAL markings be personally carried overseas. Where it is not practical to make use of the service offered by DCS, the appropriate Principal Security Adviser must be contacted, allowing 7 days notice. After confirmation by DCS that the task cannot be met by an official defence courier, the application will be endorsed and forwarded to the Foreign and Commonwealth Office for issue of a single journey casual courier passport.

04124. Except where specifically stated, paragraphs 04126-04148 do not apply to RESTRICTED documents.

04125. When travelling overseas:

a. Officers should try to remain inconspicuous.

b. Documents should be carried in a sturdy dual combination locked commercial type briefcase. Prohibited items listed in para 1 of Annex N **must not** be carried.

Note: When RESTRICTED material is carried abroad, a briefcase meeting the specifications as described above must be used.

04126. Memoranda or minutes of the Cabinet and its committees or of Ministry of Defence committees (including committees of the Chiefs of Staff), whatever their protective marking, may not normally be taken or sent out of the country. If it is essential for such papers to leave the country, permission should be sought as follows:

a. **For Cabinet and Cabinet committees.** Through Secretary of State for Defence (Private Office) for documents handled by them (ie cabinet and Ministerial committee documents and the documents of official committees where Ministry of Defence representation is at Defence Council level), and direct from the private secretary to the secretary of the Cabinet for all other official committee documents.

b. **For Ministry of Defence committees.** Through the secretary of the committee concerned. In no circumstances may Cabinet conclusions be taken or sent out of the country.

04127. Except when ministers or senior officials are travelling with a group of colleagues in British controlled transport to or from meetings in territories of countries

presenting a special security risk (see Annex C), in no circumstances will permission be given for the personal carriage of protectively marked documents (including RESTRICTED) across the borders of, within, or over, such countries.

04128. In all cases where documents marked CONFIDENTIAL or above are taken overseas, a list of the documents must be left with the dispatching establishment, a copy being held with the documents in the container carried by the courier. The establishment originating the consignment should also give notice, to the office to which the material is addressed, of the courier's travel arrangements, so that undue delay in delivery can be notified to the originating establishment for immediate investigation.

Carriage of protectively marked documents to non-NATO countries by casual couriers possessing diplomatic immunity conferred by the Foreign and Commonwealth Office

04129. Where documents are required at destinations in Non-NATO countries, every possible effort should be made to send them in advance through normal channels. Because of the additional risks entailed when carrying protectively marked documents to/from such countries by hand, Defence Courier or Queens Messenger Services should be employed where transmission in advance is not practical. Only where these services cannot meet delivery will personal carriage by staff be entertained.

04130. Written authority from the appropriate Principal Security Adviser on behalf of the PUS, is required in respect of all applications for authority to carry protectively marked material as a casual courier possessing diplomatic immunity. Authority will only be granted to officers or senior non-commissioned officers of the Services or established officials not below Administrative Officer grade, who are UK based and citizens of the United Kingdom or Commonwealth and have been vetted at the appropriate level.

04131. Applications for the personal carriage of protectively marked documents overseas, signed by the head of establishment, should be submitted IN DUPLICATE in the form shown at Annex E to this chapter to reach the appropriate Principal Security Adviser at least 7 working days before the start of the journey abroad. Applications will be referred as a matter of routine to the DCS and only forwarded to the Foreign and Commonwealth Office for their action where the former confirms that neither they nor the Queen's Messenger Service can assist.

04132. Subject to authority granted by the appropriate Principal Security Adviser, the officer who is to act as casual courier will be required to report, with the documents to be carried, to the Communications Department of the Foreign and Commonwealth Office. The courier will be briefed for the journey and provided with a special courier's passport and "diplomatic way-bill" valid for one journey only; the documents will be sealed in a diplomatic bag. The officer must be in possession of a valid British passport and visas necessary for the journey. These documents, and the properly constituted diplomatic bag, provide the courier with inviolability and immunity from

any form of arrest or detention in the country of his destination abroad and in any other countries he may pass through en route in accordance with international agreement. The diplomatic bag may not be opened, examined (eg by airport scanner) or detained by foreign authorities en route; in case of difficulty the local British representative must be contacted. However, the privilege of diplomatic immunity must not be abused by also carrying prohibited items in the diplomatic bag with protectively marked documents. A list of prohibited items is given at para 1 of Annex N.

04133. Where it is essential for ministers or senior officials (normally members of the Defence Council) travelling abroad to have access to official papers during the journey, the appropriate Principal Security Adviser should be asked to make arrangements with the Foreign and Commonwealth Office for the documents to be carried in a locked and labelled pouch or briefcase instead of in a sealed bag. (Whatever the destination, such exceptions require personal authorization by the PUS.) The requirement should be indicated when submitting a request to the appropriate Principal Security Adviser in accordance with para 04130.

> ***Note:*** The reading of protectively marked papers during journeys, whether in the United Kingdom or abroad, is essentially insecure; not only may documents be overlooked and/or mislaid but once they are out of the pouch or bag, a foreign customs officer may attempt to inspect and possibly seize them.

Carriage of protectively marked documents to NATO countries by casual couriers not possessing diplomatic immunity

04134. Where documents are needed in NATO countries at very short notice, the appropriate Principal Security Adviser may exceptionally, at their discretion and subject to the restrictions at paras 04125-04128 above, waive the need for diplomatic immunity and authorize the carriage of UK or IDO (non-accountable) documents marked CONFIDENTIAL or SECRET. Applications seeking authorization of casual couriers within these constraints, signed by the head of establishment should be sent (in the form shown at Annex E to this chapter) to the appropriate Principal Security Adviser at least 7 working days before the start of the journey abroad. Sector security authorities, at 1 star level or above, may delegate to nominated HOEs/COs authority to waive the need for diplomatic immunity, and to authorize carriage of such documents by staff subject to the restrictions at paras 04125-04128.

04135. Provided the journey does not involve travel through, to or over countries presenting a special security risk, officers may carry UK and IDO RESTRICTED documents without formal documentation as a casual courier. The documents must, however, be carried in a sturdy dual combination locked commercial type briefcase.

04136. Before authorizing carriage of documents to NATO countries with waiver of diplomatic immunity, the authorizing officer should:

a. Establish that it is essential for the document(s) to be taken out of the United Kingdom for use at a meeting in a NATO country.

b. Seek confirmation from the Foreign and Commonwealth Diplomatic Bag Service and the DCS that the documents cannot be consigned through their channels to reach the destination in time.

c. Ensure that the officer nominated is cleared for access to the information carried.

Authority to carry documents must be provided in writing (see para 04139) and be issued only by, or on behalf of, the appropriate Principal Security Adviser (see para 04134).

04137. The officer may be authorized to travel to or through the following countries, and to no others:

Belgium	Luxembourg
Canada	Netherlands
Denmark	Norway
France	Portugal
Germany	Spain
Greece	Turkey
Iceland	United States
Italy	

04138. To reduce security hazards the preferred method of travel is by United Kingdom Service or civil aircraft. However aircraft of one of the countries listed in para 04137 may be used. SECRET documents are not to be carried on foreign airlines unless authority to do so has been granted by the appropriate Principal Security Adviser. The Authorizing Officer should always select practicable means of travel with due regard to the current threat of hijacking of aircraft (see paras 04146 – 04148 and Annex I).

04139. Authorization under these rules must be in the form of Annex F, prepared in duplicate, and signed by an officer to whom powers have been delegated by the appropriate Principal Security Adviser (normally not below the rank of Assistant Secretary or 1 star equivalent). The duplicate copy of each authorization should be retained by the establishment security officer and made available for inspection by security staff. Officers intending to carry documents must be issued with a set of instructions, as detailed in Annex G, and must certify in writing, as in Annex H, that they have read and understood them before departure.

04140. Authorization for carriage under the rules set out in this section is limited solely to the transmission of UK, non-accountable NATO CONFIDENTIAL and SECRET documents and UN documents (See Annex L). Documents bearing additional markings should not be carried without reference to the appropriate Principal Security Adviser or to the delegated officer. Provided the journey does not involve travel through, to or over any non-NATO countries, UK and NATO RESTRICTED

documents may be carried without authority. Such documents must, however, be carried in a sturdy dual combination locked commercial type briefcase. The personal carriage of documents protectively marked UK or NATO CONFIDENTIAL or SECRET to non-NATO countries and the carriage of UK TOP SECRET material overseas to NATO and non-NATO countries, must be in accordance with para 04129-04133. Guidance on the international transmission of accountable material, eg, that bearing marking, ATOMAL, COSMIC and WEU, is contained in Section IV of this Chapter. These rules generally prohibit personal hand carriage, recommending official transmission via the controlling authority concerned. Further details will be found in the appropriate instructions or by contacting the relevant controlling office. Two copies of the list of documents to be carried must be prepared one to be retained in the establishment and the other packed with the documents.

04141. Documents must be carried under cover. The cover, securely sealed in accordance with the rules contained in Section II, must be addressed to the officer himself care of his destination. The cover must bear the reference number of the Certificate of Authorization (Annex F), the departmental stamp and the signature of the officer who signed the Authorization Certificate. The package must be carried in a sturdy dual combination locked commercial type briefcase or similar container of a type meeting the approval of the relevant security regulations.

04142. Authority under these rules will be given only in respect of documents required at a meeting, subject to the conditions addressed in paragraph 04138. Agreements on security with other countries generally provide that protected information may only be exchanged on a Government-to-Government basis or between international organisations concerned. Protectively marked documents should, therefore, not be handed directly to representatives of overseas firms but where necessary, released to a Government Department of the country concerned, or to the local British Embassy or High Commission, for onward transmission. Receipts should be obtained where necessary.

04143. On conclusion of a visit and whenever practicable, documents should be returned to the United Kingdom by diplomatic bag through the local British Embassy, High Commission or Consular Office. If personal hand carriage is necessary on the return journey, the carrier must be provided, before the outward journey, with the necessary documents, - ie, spare envelope(s) bearing the same reference number, stamp and signature as used on the outward journey and materials for resealing the package(s). The return journey must also be noted in the original authorization.

> ***Note:*** Where an officer (who is not a casual courier) attends a meeting overseas and has reason to believe he/she may be required to bring back protectively marked documents to the United Kingdom, the officer should arrange with the British Embassy, High Commission or Consular Office for his/her documentation as a casual courier. Facilities for sealing the documents should be sought, and a sturdy dual combination lock commercial type briefcase or other suitable official container used to transport the documents to the UK.

04144. On return the casual courier should personally verify with the officer holding the duplicate lists of material removed that all documents have been returned or receipts

obtained. The casual courier should also send his Authorization Certificate to his security officer. Any incidents of possible security significance that occurred during the journey should be reported to the security officer.

04145. Under no circumstances should a NATO Travel Order be used as authority to carry protectively marked documents overseas.

Precautions against hijacking

04146. Where HOE have been given the authority to authorize members of their staffs to act as casual couriers of documents to, or through the countries listed in para 04140, due regard must be given to the threat of hijacking of aircraft. This requires the exercise of judgement on each occasion, weighing the necessity for personal carriage of each document against the risks entailed.

04147. Any difficulties arising out of the implementation of para 04146 should be referred to the appropriate Principal Security Adviser.

04148. Because of precautions taken by airline authorities, both at home and overseas, to minimise the hijacking of aircraft on international flights the additional instructions in Annex I should, until further notice, be issued to officers acting as casual couriers.

Carriage of protectively marked material overseas by Service personnel acting as Casual Couriers during emergency operations

04149. It is recognised that there are times when protectively marked material is required urgently in an operational non-NATO theatre and the Services needs cannot be met by the use of the DCS or the QMS of the FCO. An example of this is the no-notice deployment of aircraft/ships/support personnel in an out of area operation to non-NATO countries.

04150. Only in such exceptional circumstances may Sector security staff authorise, at their discretion, an officer to carry material protectively marked up to SECRET without diplomatic immunity. Where descriptors, codewords or caveats are included in the marking then the approval of the appropriate Principal Security Adviser (at the appropriate level) should be sought. Such Casual Couriers travelling under this facility may be subject to Customs and security checks.

04151. Casual Couriers must not carry NATO documents to the following countries without the permission of the appropriate NATO authority:

Australia	Austria
Japan	Sweden
Switzerland	New Zealand

Countries with special security risks

04152. Casual couriers should not be used to carry protectively marked material to the following countries unless authorised by the Director/Head of the appropriate Principal Security Adviser and then only if all efforts to secure diplomatic immunity for the proposed courier has failed.

Afghanistan	Belarus	China (inc Hong Kong SAR, Tibet and Macao)
Cuba	Iran	Iraq
Lebanon	Libya	North Korea
Russia	Sudan	Syria
Ukraine	Vietnam	Yugoslavia (Serbia and Montenegro)

Note: Travel by the airlines of the above countries should be avoided where possible but may be allowed after due consideration of the risks which may attract to the courier as well as the material he/she is carrying.

04153. PSyA staff should check with the FCO for the latest travel advice on all countries before authorisation is given. The Casual Courier should also be briefed on the dangers of hijacking and given a copy of the guidance at Annex I.

04154. PSyA staff must ensure that the Casual Courier is:

a. Cleared for access to the material carried;

b. Issued with instructions (Annex G) which he/she should certify as having read and understood;

c. Carrying a written authorisation in the form of Annex F; and

d. Provided with a list of documents to be carried. A second copy should be retained by the ESyO/USO/BSO.

Return to the UK

04155. On return the Casual Courier should personally verify with the officer holding the duplicate list of material removed that all documents have been returned or receipts obtained.

Removal of protectively marked documents between official premises during office relocation

04156. Normally branches will be relocated under arrangements whereby a contractor and its staff who are cleared to handle up to and including SECRET will be involved. Such relocations will in all likelihood also involve the movement of office furniture, ordinary and security containers and computer equipment. Documents up to and including SECRET should be moved in accordance with the details shown below; the

movement of TOP SECRET and other documents where only bags and small boxes are involved is covered at para 04157.

a. RESTRICTED, CONFIDENTIAL and SECRET documents should be packed in crates (to be supplied by contractors with lids which have holes in capable of being fastened by the use of plastic ratchet ties). Plastic ratchet ties, which can be removed only by cutting, with a tag showing a serial number, should be used. A list of the contents of each crate is to be maintained, detailing RESTRICTED, CONFIDENTIAL and SECRET material. The serial numbers on each tie should be noted before and after shipment, to ensure that tampering has not taken place. In the event of evidence of tampering and possible compromise having taken place, the appropriate Principal Security Adviser should be notified in accordance with sub para l below.

b. A list containing details of consignment (as required by sub-para 04156a above) should be sent either in advance to the final destination, or given in a sealed envelope to the driver or crew of the commercial vehicle with instructions to hand it over to the staff at the delivery point.

c. Driver and crew should be given no indication of the protective marking or subject of the items.

d. Stick-on labels giving details of contents and protective markings must not be used.

e. During loading and unloading, staff must ensure that crates containing protectively marked documents are not left unsupervised.

f. Where possible, the transmission of documents is to be completed in one move and vehicles must be manned at all times. When an overnight stop is involved, vehicles must be parked on guarded premises subject to prior MOD approval.

g. Driver and crew should be advised if any crates include fragile items ie computers, etc. (The appropriate Sector IT security staff should be consulted regarding relocation of computers).

h. Vehicles must have secure cargo areas where the only form of entry is through lockable doors. Rear doors (ie main access to secure cargo area) of vehicles are to be locked with an approved security padlock or with a good quality padlock. Advice on locks and padlocks can be obtained from the appropriate Sector security staff. Arrangements should be made to ensure that one key is held by the relevant MOD officials at both the sending and receiving points of the journey, unless the load is escorted by MOD staff, who are insured to travel in the commercial vehicle.

i. The driver is to be given a contact number to alert a relevant area in MOD capable of organising remedial action in the event of a breakdown.

j. Separate instructions should be given to the driver on action to be taken in the event of a traffic accident, or emergency. The instruction should identify circumstances in which the vehicle may be unloaded and action to be taken to record the transfer of crates, etc.

k. The guard Forces at both the pickup and delivery points should be informed of the crew and vehicle details and time of departure and arrival.

l. Contents to be checked by staff on arrival, or as soon as possible and to advise the appropriate Principal Security Adviser if a compromise has taken place.

Further detailed advice on the above can be obtained from the appropriate Principal Security Adviser at an early stage.

04157. Branches that have quantities of TOP SECRET, ATOMIC or other documents requiring special handling must send them separately through the DCS or by MOD Mail Service (MMS). DCS/MMS will also move bags or boxes containing documents marked up to SECRET provided the weight of each bag or box does not exceed 15Kg. Documents will be moved on existing routes although special tasks can be undertaken with prior consultation.

Homeworking

04158. Homeworking is defined as the use of a person's home as their normal place of work and requiring access to/retention of official information. It is often described as working **from** home. It should not be confused with working **at** home, which is the term used to describe something which is strictly on a temporary basis eg during transport disruptions or for overnight working (see para 04113).

04159. Homeworking entails special security risks and will only be allowed following consideration, on a case by case basis by line management, the appropriate personnel management authority and Sector security staff.

04160. The specific security rules which apply to homeworking are shown at Annex M.

SECTION IV

SPECIAL MARKINGS

04161. Only those with a need to know, or need to hold, should have access to protectively marked information. When it is necessary to provide additional protection by reinforcing the "need to know" principle, special markings that restrict access should be used, normally in conjunction with a protective marking. Special markings consist of:

a. **National caveats.** National caveats exist for the additional protection of certain types of protectively marked UK material, eg UK EYES ONLY, CANUKUS EYES ONLY. Definitions of these and other recognized caveats, and advice on their use, are given in Chapter 16.

b. **Descriptors.** Descriptors help to implement the "need to know" principle by indicating the nature of the asset's sensitivity and the need to limit access accordingly. A list of MOD descriptors is at Annex J.

c. **Additional markings.** Additional markings may be required to ensure the special handling of some material to indicate particular aspects of ownership, issue or release, eg Compartmented or Codeword material. Further information concerning Compartments, Codewords and nicknames are at Annex K.

d. **International defence organisation (IDO) markings.** IDOs, eg the North Atlantic Treaty Organisation (NATO) and the Western European Union (WEU) and their member nations, use similar protective markings, known as classifications, to the UK and prefixed NATO or WEU as appropriate. Further details are at Annex L.

This page intentionally left blank

ANNEX A TO CHAPTER 4

EXAMPLE OF MOD F 672

MOD Form 672

Record of Protectively Marked Documents (TOP SECRET and SECRET) contained in:-

File Number

This card should be kept on the LEFT hand side of the file as the top enclosure.

Encl. No.	Document Reference No.	Date of Document	Copy No.	Protective Marking	Date of Downgrading

Note: The reverse of the form is also ruled in columns as above.

This page intentionally left blank.

APPENDIX 1 TO
ANNEX A TO
CHAPTER 4

EXAMPLE OF MOD F 171

MOD FORM 171

Part 1 - Request for Downgrading of Protectively Marked Documents

To:	From:

It is requested that authority be given for the downgrading of the documents listed overleaf. If downgrading is agreed, please state new protective marking in column (e); otherwise insert "No change".

Date..... Signature.....

Part 2 - Authority to Downgrade Protectively Marked Documents

To:	From:

Please note that the documents listed below should now be graded as shown in column (e)

(a) Reference No.	(b) Description (i.e. File, letter, report etc.)	(c) Date	(d) Present protective marking	(e) Revised protective marking

Date..... Signature..... Grade.....

APPENDIX 2 TO ANNEX A TO CHAPTER 4

Serial No: **Original** **MOD Form 924**

Authority for and notification of the removal of documents marked CONFIDENTIAL and above from official premises to destinations in the United Kingdom

Before completing this form, read the relevant paragraphs of DMS Vol 1, and the notes on the cover of this pad.

Part A: Authorising officer

Officer's name:

Rank/grade: **Branch:**

Part B: Destination, date(s) and reason for removal of documents

The documents listed at Part C are to be removed to

on for the purpose of

Part C: Documents removed

Reference of document/file (a)	Last encl/minute numbers (files only) (b)	Protective marking (c)

Part D: Authority to remove documents

Authority is given to remove the documents listed at Part C from official premises for the reason stated at Part B. The officer named in Part A is aware that the documents removed must be carried in accordance with current security regulations and remain in his/her custody at all times unless placed in secure storage under officially approved arrangements.

Signature Name (Block letters) Date

Head of Establishment

Part E: Certificate of return of documents

Complete duplicate only

Serial No: **Duplicate** **MOD Form 924**

Authority for and notification of the removal of documents marked CONFIDENTIAL and above from official premises to destinations in the United Kingdom

Before completing this form, read the relevant paragraphs of DMS Vol 1, and the notes on the cover of this pad.

Part A: Authorising officer

Officer's name:

Rank/grade: **Branch:**

Part B: Destination, date(s) and reason for removal of documents

The documents listed at Part C are to be removed to

on for the purpose of

Part C: Documents removed

Reference of document/file (a)	Last encl/minute numbers (files only) (b)	Protective marking (c)

Part D: Authority to remove documents

Authority is given to remove the documents listed at Part C from official premises for the reason stated at Part B. The officer

named in Part A is aware that the documents removed must be carried in accordance with current security regulations and remain in his/her custody at all times unless placed in secure storage under officially approved arrangements.

Signature Name (Block letters)

Date Head of Establishment

Part E: Certificate of return of documents (Duplicate only)

I certify that all documents listed at Part C were returned to the office on date

Signature Name (block letters)

Branch

ANNEX B TO

CHAPTER 4

OFFICE SECURITY CHECK SHEET

Room..... Month.....

The undersigned certifies that:

1. All security containers are securely locked and security keys mustered.

2. No protectively marked papers, waste, security keys, computer media or other protected material has been left accessible to unauthorised persons.

3. All photocopiers, computers and facsimile machines have been switched off, hard disks removed (if applicable) and power supplies secured.

Date	Time	Signature	Date	Time	Signature

Completed forms should be returned to the establishment security officer.

This page intentionally left blank

APPENDIX 1 TO
ANNEX B TO
CHAPTER 4

SPOT CHECK REPORT

Date and Time

Establishment.....……. ……..……. checking started

1. I selected the following documents at random from the protected document register (PDR)(MOD F 102), file index etc, for checking in accordance with DMS Vol 1 Chapter 4. Loose documents (as distinct from files/folders - see para 2 below) together with any annexes and appendices were checked for completeness.

Serial	PDR serial No	Doc ref	Doc date	Protective marking	Location of doc (if held, quote file no)	Remarks #
	(i)	(ii)	(iii)	(iv)	(v)	(vi)
a.						
b.						
c.						
d.						
e.						
f.						

2. Of the files/folders listed above, I checked the TOP SECRET and SECRET contents of the following, page by page and against the entries on the minute or inventory sheets.

a. _____
b. _____
c. _____

3. In the course of my check I found:

* No irregularity/difficulty.
* Irregularities/difficulties which are the subject of the report overleaf.

Date and time check completed……Signed……

Rank/Grade……Name in Capitals……

Notes:

1. A spot check should cover all PDRs.
2. If a document or receipt is produced insert "Seen", if not, insert "Not Seen" and report action taken overleaf.
3. * Delete as appropriate.
4. No other record of this check should be made either on the documents themselves or in any supporting register or index/inventory.

ANNEX C TO CHAPTER 4

TRANSMISSION OF PROTECTED DOCUMENTS

General

1. These instructions provide guidance for the transmission of all types of protected and unclassified documents **except**:

a. ATOMIC, COSMIC, ATOMAL, FOCAL, CRYPTOGRAPHIC and STRAP material;

b. Cabinet/Ministerial committee documents;

c. Documents subject to special handling arrangements notified separately to those with a need to know.

***Note*:** Envelopes, packages, etc, reaching the mail room which do not comply with instructions in this Annex will be returned to the originator. If necessary, mail will be opened to identify the originator.

2. The instructions are broken down by security protection, and destination as follows:

Protective Marking Destination	**TOP SECRET**	**SECRET**	**CONFIDENTIAL**	**RESTRICTED/ UNCLASSIFIED**
Within the same location or to another listed location inc OGDs	Appendix 1	Appendix 2 Section I	Appendix 3 Section I	Appendix 4 Section I
To Embassies and High Commissions in Central London	Appendix 1	Appendix 2 Section II	Appendix 3 Section II	Appendix 4 Section II
To other postal addresses in the UK **excluding Northern Ireland**	Appendix 1	Appendix 2 Section III	Appendix 3 Section III	Appendix 4 Section III
To diplomatic posts abroad	Appendix 1	Appendix 2 Section IV	Appendix 3 Section IV	Appendix 4 Section IV
To other addresses overseas **and to Northern Ireland**	Appendix 1	Appendix 2 Section IV	Appendix 3 Section IV	Appendix 4 Section IV

***Note*:** For transmission purposes CRYPTOSECURITY documents and cypher logs are always to be treated as TOP SECRET and sent under cover of MOD Form 488 (see Appendix 1)**.**

Use of Defence Mail Service

3. The Defence Postal and Courier Service (DPCS) operates a dedicated mail service to a number of Service and civilian organisations throughout the country. The majority of these locations are organised in a manner that allows simplified procedures to be followed when despatching protected documents to them. Details of the locations served by the Defence Mail Service, indicating those between which transmission of SECRET and CONFIDENTIAL is permissible using a single envelope (without protective marking), is published periodically in JSP 367 to which despatching organisations should refer. Advice on the latest list can be obtained from the DPCS.

Use of the Diplomatic Bag for Transmission of Material to Diplomatic Posts Overseas

4. Rules for preparation of mail for despatch via diplomatic bag are described in paras 04097 - 04101. In all cases, mail must be addressed as detailed in Appendices to this Annex.

5. All mail originating from DIS branches (with a protective marking of CONFIDENTIAL and above) addressed to diplomatic posts abroad MUST be despatched by diplomatic bag.

6. All official mail, (other than unclassified publicity and information material) for diplomatic posts in the following countries is also to be sent by diplomatic bag:

Afghanistan	Libya
Albania	Mongolia
Belarus	North Korea
Bulgaria	Romania
Cambodia	Russia (The Federation)
Cuba	South Africa
Iran	Syria
Iraq	Ukraine
Laos	Vietnam

Envelopes containing TOP SECRET or SECRET material addressed to these locations are to be transmitted in Keepsafe envelopes or sealed, if still available, with high security tape; similarly addressed parcels and packages must be **wafer-sealed** (see para 04077).

Unreliable Postal Services

7. Detailed information on current rules for transmission of RESTRICTED or Unclassified mail via diplomatic bag, eg to countries with unreliable postal services, is provided by DCS in JSP 367.

This page intentionally left blank

APPENDIX 1 TO ANNEX C TO CHAPTER 4

TRANSMISSION OF TOP SECRET DOCUMENTS FROM ANY MOD OR SERVICE LOCATION IN THE UK TO ANY ADDRESSEE

WARNING

1. TOP SECRET documents must never be transmitted through Post Office or other non-official channels. They must travel hand-to-hand, receipted.

2. TOP SECRET documents must never be over-covered so that their protective marking is obscured.

3. For transmission purposes, CRYPTOSECURITY material and cypher logs are always to be treated as TOP SECRET.

4. Where IDO material is to be transmitted, the marking "COSMIC" or "FOCAL" (as appropriate) is to be inserted on MOD Form 488 to appear in front of the marking TOP SECRET.

5. Approval must be obtained from InfoSy(Industry)1 or Command HQs before TOP SECRET documents are transmitted to a foreign or Commonwealth-based defence contractor.

6. TOP SECRET documents are only to be sent to private addresses in exceptional circumstances and with specific permission from PUS. They are not to be sent to addresses where foreign servants are employed or where there is no suitable container in which to keep them (see paras 04093 - 04094).

7. Envelopes or packages, etc, in transit must never be left unattended.

8. Use of Keepsafe security envelopes is permitted.

Preparation for Normal Despatch

1. Select one unused envelope of suitable size and apply a legible stamp identifying the despatching organisation, eg. a branch stamp.

2. Prepare MOD Form 488 (special TOP SECRET label), addressing it personally to an officer by name or appointment and correct address. Include the reference and date of origin of the document to be enclosed.

3. For addresses within approved locations served by the Defence mail service (see para 3 of Annex C), the address must include the building and room number (for locations outside London, the name of the town/city should also be included). The post code must not be included.

4. For diplomatic posts abroad, Service and international organisations served by BFPO numbers, include the words:

"c/o LCT, BFPO 1000".

5. For all addressees overseas, add the words "Certified Official", this being endorsed by an authorising officer.

6. For ships in UK or overseas ports or waters, include the words:

"HMS ...., c/o BFPO 999."

7. If the document bears a National caveat, eg "UK EYES ONLY", this must not appear on the label; the label must be addressed "Exclusive to" the addressee by name and appointment.

8. Prepare receipt (MOD Form 24) and insert, with the document, into the envelope and proceed as follows:

a. Unused envelope: affix MOD Form 488 already prepared to the envelope and seal in accordance with Appendix 5;

or

b. Keepsafe security envelope: affix MOD Form 488 already prepared to the envelope flap and seal in accordance with para 04073.

***Note*:** Parcels, packages, etc, must be sealed using wafer seals (see para 04077).

Normal Despatch

9. Sealed envelopes are to be conveyed by hand to the central registry, where they will be recorded and inserted in an outer cover for further transmission. The carrier is to give and take timed receipts (MOD Form 32) bearing the despatcher's room number and stamp.

Despatch using Locked Pouches, etc

10. Locked pouches, etc, are to be sent direct by hand of carrier as described at para 2 above. Documents transmitted in a locked pouch or box need not be enveloped unless recipient is to forward them to a third party; a receipt (MOD Form 24 or equivalent - see para 04078) is to be attached to each loose TOP SECRET document to be placed in the pouch; the pouch is to be addressed to the intended recipient personally by name and/or appointment. (Key-holders are responsible for onward transmission (taking appropriate safeguards) of any documents received which are not of their concern).

This page intentionally left blank

APPENDIX 2 TO ANNEX C TO CHAPTER 4

TRANSMISSION OF SECRET DOCUMENTS

SECTION I

TRANSMISSION WITHIN MOD OR SERVICE BUILDINGS/SITES OR BETWEEN APPROVED LOCATIONS (INCLUDING OTHER GOVERNMENT DEPARTMENTS) SERVED BY THE DEFENCE MAIL SERVICE (SEE PARA 3 OF ANNEX C)

WARNING

1. Envelopes or packages in transit must never be left unattended.

2. Mail to other Government departments in Central London not served by the Defence mail service (see para 3 of Annex C) should be despatched in accordance with Section III.

Preparation for Normal Despatch

1. If the document is to be sent outside the building/site, prepare and affix a receipt (MOD Form 24) (see para 04078).

2. Select one unused envelope (or unused wrappings), or an envelope of good quality to be used with an economy label, of suitable size and apply a legible stamp identifying the despatching organisation (eg. a branch stamp).

3. Address the envelope/package by name and/or appointment/branch plus room number and building/establishment. For locations outside central London, the address should include the appropriate town, eg. Royal Military Academy, Woolwich. The postcode must not be included.

4. If the document bears a National caveat, eg. "UK EYES ONLY", the envelope is to be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope, etc.

5. The security marking of contents **must not** be shown on the envelope/package; descriptor markings, eg. "STAFF" may be shown.

6. Insert the document (and receipt if appropriate) and stick down the flap (or pack the document sticking down all seams).

7. Mark envelope "Defence mail service only".

Normal Despatch

8. Sealed envelopes or packages should be placed in the "out" tray for collection by transit services.

Despatch using Locked Pouches, etc

9. Documents transmitted in a locked pouch or box, destined for an addressee outside the building/site, need not be enveloped unless the recipient is to forward them to a third party. A receipt (MOD Form 24 or equivalent (see para 04078) is to be attached to each loose SECRET document or set of documents to be placed in the pouch. The pouch is to be addressed to the intended recipient personally by name and/or appointment. (Key-holders are responsible for onward transmission (taking appropriate safeguards) of any documents received which are not of their concern). Pouches, etc should be conveyed by hand or despatched through normal transit services.

SECTION II

TRANSMISSION TO EMBASSIES AND HIGH COMMISSIONS IN CENTRAL LONDON SERVED BY THE DEFENCE MAIL SERVICE FROM APPROVED LOCATIONS ALSO SERVED BY THE DEFENCE MAIL SERVICE (SEE PARA 3 OF ANNEX C)

WARNING

1. Envelopes or packages in transit must never be left unattended.

Preparation for Normal Despatch

10. Prepare and affix a receipt (MOD Form 24) to the document.

11. **Inner envelope/wrapping.** Select one unused envelope (or unused wrapping) of suitable size and apply a legible stamp identifying the despatching organisation (eg. a branch stamp) and the reference and date of origin of the document to be enclosed.

12. Address the envelope/package by name and/or appointment/branch plus room number and name of Embassy/High Commission. If the document bears a National caveat, eg. "UK/US EYES ONLY", the envelope/package is to be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope/package.

13. Mark "SECRET" boldly in red above and below the address; the protective marking should be prefixed "WEU" or "NATO" if the contents are so marked.

14. Insert the document (and receipt) and stick down the flap (or pack the document sticking down all seams).

15. **Outer envelope/wrapping.** Select a second unused envelope (or unused wrappings) and apply the address as at para 12 above. "PO Box 701, London WC2H 8BG" should be used as a return address; a branch stamp should **not** be used.

16. Insert the first envelope/package and stick down the flap (or pack sticking down all seams).

17. Mark envelope "Defence mail service only".

Normal Despatch

18. Sealed envelopes or packages should be placed in the "out" tray for collection by transit services.

Despatch using Locked Pouches, etc

19. Documents transmitted in a locked pouch or box need not be enveloped unless the recipient is to forward them to a third party; a receipt (MOD Form 24 or equivalent - see para 04078) is to be attached to each loose SECRET document or set of documents to be placed in the pouch. The pouch is to be addressed to the intended recipient personally by name and/or appointment. (Key-holders are responsible for onward despatch (taking appropriate safeguards) of any documents received which are not of their concern.) Pouches, etc should be conveyed by hand or through normal transit services.

SECTION III

TRANSMISSION TO ADDRESSES IN THE UK OTHER THAN THOSE COVERED IN SECTION I & SECTION II OF APPENDIX 2 AND EXCLUDING NORTHERN IRELAND (SEE SECTION IV) FROM ANY MOD OR SERVICE LOCATION IN THE UK

WARNING

1. **Envelopes and packages containing SECRET material must be prepared for despatch by one of the following approved mail services:**
   a. **Parcelforce 10, 12 or 24**
   b. **Special Delivery Service**

2. SECRET documents are only to be sent to private addresses in exceptional circumstances and with specific permission from a Head of Establishment. They are not to be sent to addresses where foreign servants are employed or where there is no suitable container in which to keep them (see para 04093 - 04094).

3. Envelopes or packages in transit must never be left unattended.

Preparation for Normal Despatch

20. Prepare and affix a receipt (MOD Form 24) to the document.

21. Inner envelope/wrapping. Select one unused envelope (or unused wrappings) of suitable size and apply a legible stamp identifying the despatching organisation (eg. a branch stamp) and the reference and date of origin of the document to be enclosed.

22. Address the envelope/package by name and/or appointment/branch and full postal address. If the document bears a National caveat, eg. "UK EYES ONLY", the envelope/package is to be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope/package.

23. Mark "SECRET" boldly in red above and below the address; the protective marking should be prefixed "WEU" or "NATO" if the contents are so marked.

24. Insert the document (and receipt) and stick down the flap (or pack the document sticking down all seams).

25. **Outer envelope/wrapping.** Select a second unused envelope (or unused wrappings).

26. For mail to official addresses, apply the address as at para 22 above.

27. For mail to private addresses, use a plain envelope; address by name without reference to rank, decorations, appointment, etc.

28. Insert the first envelope/package and stick down the flap (or pack sticking down all seams).

> ***Note*:** The outer envelope/wrapping **must not** bear any security markings, branch stamp, or other markings which might associate it with the Department. "PO Box 701, London WC2H 8BG" should be shown as the return address.

29. Mail for ships in UK ports or home waters should be addressed to

"HMS….., c/o BFPO 999."

30. Mark the envelope/package with the appropriate approved mail service in the top left hand corner.

Normal Despatch

31. Sealed envelopes or packages should be placed in the "out" tray for collection by transit services.

SECTION IV

TRANSMISSION TO DIPLOMATIC POSTS ABROAD, AND OTHER ADDRESSES OVERSEAS INCLUDING NORTHERN IRELAND FROM ANY MOD OR SERVICE LOCATION IN THE UK

WARNING

1. In no circumstances may Post Office services be used for transmission of SECRET material to Northern Ireland or to other overseas locations.

2. Envelopes or packages in transit must never be left unattended.

3. SECRET material for foreign or Commonwealth Governments or their defence contractors may only be transmitted to those countries approved by the RMIPC, and then only via the appropriate British Diplomatic post.

4. Approval must be obtained from InfoSy(Industry)1/Command HQs before SECRET mail is sent (via the appropriate British Diplomatic post) to a foreign or Commonwealth-based defence contractor.

5. The appropriate MOD Form 189 (condition of release stamp) or statement of release (Annex C to Chapter 11 of JSP 440 Volume 1) must be firmly attached to each SECRET document sent to a foreign or Commonwealth Government, or defence contractor of that country. The prefix "UK" or, where appropriate, "NATO" or "WEU", should appear before the protective marking on the document.

6. The use of Keepsafe security envelopes is permitted.

Preparation for Normal Despatch

32. Prepare and affix a receipt (MOD Form 24) to the document. In addition, a completed despatch Note (see Appendix 6) should be attached to documents intended for transmission to foreign or Commonwealth Governments or their defence contractors.

***Note* 1:** For the transmission of mail to foreign or Commonwealth Governments or their defence contractors (sent via the appropriate British Diplomatic Post), see para 42.

***Note* 2:** For the transmission of mail to British Defence Attaches/Advisers and to addresses in Northern Ireland, see para 33.

***Note* 3:** For the transmission of mail to British officers or civilians serving in international organisations, see para 55.

***Note* 4:** For the transmission of mail to HM Ships in overseas ports or waters, see para 64.

Mail to British Defence Attaches/Advisors, BDS Washington and BFPO addresses including Northern Ireland

33. **Inner envelope/wrapping.** Select one unused envelope (or unused wrappings) of a suitable size. Apply a legible stamp identifying the despatching organisation (eg a branch stamp) and the reference and date of origin of the document to be enclosed.

34. Address the envelope/package to the British Defence Attache/Adviser by name or appointment, with full address of the diplomatic post. For mail to Northern Ireland, address envelope as appropriate.

35. If the document bears a (composite) National caveat, eg "UK/US EYES ONLY", the envelope/package must be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelopment/package.

36. Mark "SECRET" boldly in red above and below the address; the protective marking should be prefixed "UK", "NATO" or "WEU" if the contents are so marked.

37. Mark the envelope/package "Certified Official", this being endorsed by an authorising officer (see para 04099).

38. Insert document and receipt (MOD Form 24) and seal the flap and seams of the envelope with high security tape as described at Appendix 5.

39. If a Keepsafe security envelope is used - seal in accordance with para 04073.

40. Packages - seal using wafer seals (see para 04078).

41. **Outer envelope/wrapping:**

a. For mail emanating from approved locations served by the Defence mail service (see para 3 of Annex C):

(1) Select an unused envelope (or unused wrappings).

(2) Apply legible stamp identifying the despatching organisation (eg a branch stamp), and address to "LCT, BFPO 1000". No protective marking is to appear on the envelope/package.

(3) Insert inner envelope/package and seal the flap (or pack sticking down all seams).

(4) Despatch as described in para 76 below.

b. For mail emanating from other locations:

(1) Select an unused envelope (or unused wrappings).

(2) Apply a legible stamp identifying the despatching organisation (eg a branch stamp), and address to "LCT, BFPO 1000". **NO** protective marking is to appear on the envelope.

(3) Insert inner envelope/package, seal the flap (or pack sticking down all seams).

(4) Mark the envelope/package with the appropriate approved mail service (Parcelforce 10, 12 or 24 or Special Delivery Service) in the top left-hand corner.

(5) Despatch as described in para 76 below.

Mail to Foreign or Commonwealth Governments or their Defence Contractors (sent via the appropriate British Diplomatic Post)

42. **First envelope/wrapping.** Select one unused envelope (or unused wrappings) of a suitable size.

43. Address the envelope/package by name and/or appointment/branch and full postal address of the foreign or Commonwealth government. Apply the reference and date of origin of the document to be enclosed. If the document bears a (composite) National caveat, eg. "UK/US EYES ONLY", the envelope/package must be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope/package.

44. Mark "SECRET" boldly in red above and below the address; the protective marking should be prefixed "UK", "NATO", or "WEU" if the contents are so marked.

45. Insert the document and receipt (MOD Form 24) and despatch note (see Appendix 6). Do **not** seal the flap of the envelope; packages should be **loosely** secured, ie, do not stick down seams.

46. **Second envelope/wrapping.** Select a second unused envelope (or unused wrappings) of a suitable size. Apply a legible stamp identifying the despatching organisation (eg a branch stamp) and the reference and date of origin of the document to be enclosed.

47. Address the envelope/package to the British Defence Attache/Adviser by name or appointment, with full address of the diplomatic post.

48. If the document bears a (composite) National caveat, eg "UK/US EYES ONLY", the envelope/package must be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope/package.

49. Mark "SECRET" boldly in red above and below the address; the protective marking should be prefixed "UK", "NATO" or "WEU" if the contents are so marked.

50. Mark the envelope/package "Certified Official", this being endorsed by an authorising officer (see para 04099).

51. Insert first unsealed envelope/loosely secured package and seal the flap and seams of the envelope with high security tape as described at Appendix 5.

52. Keepsafe security envelope - seal in accordance with para 04073.

53. Packages - seal using wafer seals (see para 04078).

54. **Third (outer) envelope/wrapping:**

a. For mail emanating from approved locations served by the Defence mail service (see para 3 of Annex C):

(1) Select an unused envelope (or unused wrappings).

(2) Apply legible stamp identifying the despatching organisation (eg a branch stamp), and address to "LCT, BFPO 1000". **No** protective marking is to appear on the envelope/package.

(3) Insert second envelope/package and seal the flap (or pack sticking down all seams).

(4) Despatch as described in para 76 below.

b. For mail emanating from other locations:

(1) Select an unused envelope (or unused wrappings).

(2) Apply a legible stamp identifying the despatching organisation (eg a branch stamp), and address to "LCT, BFPO 1000". **No** protective marking is to appear on the envelope.

(3) Insert second envelope/package, seal the flap (or pack sticking down all seams).

(4) Mark the envelope/package with the appropriate approved mail service (Parcelforce 10, 12 or 24 or Special Delivery Service) in the top left-hand corner.

(5) Despatch as described in para 76 below.

Mail to British officers or Civilians serving in International Organisations

55. **Inner envelope/wrapping.** Select one unused envelope (or unused wrappings) of a suitable size. Apply a legible stamp identifying the despatching organisation (eg a branch stamp) and the reference and date of origin of the document to be enclosed.

56. Address the envelope/package by name and appointment with postal address (as appropriate) as follows:

Within SHAPE	-	"c/o UKNMR, SHAPE, BFPO 26"
Within NATO	-	"c/o UK Delegation to NATO, (Brussels area) Brussels, BFPO 49"
Within SACLANT	-	"c/o UKNLR to SACLANT, HMS SAKER, BFPO 2"
Within WEU	-	"c/o British Embassy, Paris"

57. If the document bears a (composite) National caveat, eg "UK/US EYES ONLY", the envelope/package must be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope/package.

58. Mark "SECRET" boldly in red above and below the address; the protective marking should be prefixed "UK", "NATO", or "WEU" if the contents are so marked.

59. Mark the envelope/package "Certified Official", this being endorsed by an authorising officer (see para 04099).

60. Insert document and receipt (MOD Form 24) and seal the flap and seams of the envelope with high security tape, if still available, as described at Appendix 5.

61. If a Keepsafe security envelope is used seal in accordance with para 04073.

62. Packages - seal using wafer seals (see para 04078).

63. **Outer envelope/wrapping:**

a. For mail emanating from approved locations served by the MOD mail service (see para 3 of Annex C):

(1) Select an unused envelope (or unused wrappings).

(2) Apply legible stamp identifying the despatching organisation (eg a branch stamp), and address to "LCT, BFPO 1000". **No** protective marking is to appear on the envelope/package.

(3) Insert inner envelope/package and seal flap (or pack sticking down all seams).

(4) Despatch as described in para 76 below.

b. For mail emanating from other locations:

(1) Select an unused envelope (or unused wrappings).

(2) Apply a legible stamp identifying the despatching organisation (eg a branch stamp), and address to "LCT, BFPO 1000". **No** protective marking is to appear on the envelope.

(3) Insert inner envelope/package, seal the flap (or pack sticking down all seams).

(4) Mark the envelope/package "Parcelforce 24" in the top left-hand corner.

(5) Despatch as described in para 76 below.

Mail to HM Ships in Overseas Ports or Waters

64. **Inner envelope/wrapping.** Select one unused envelope (or unused wrappings) of a suitable size. Apply a legible stamp identifying the despatching organisation and the reference and date of origin of the document to be enclosed.

65. Address the envelope by name and/or appointment to "HMS..."

66. If the document bears a (composite) National caveat, eg "UK/US EYES ONLY", the envelope/package must be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope/package.

67. Mark "SECRET" boldly in red above and below the address; the protective marking should be prefixed "UK", "NATO", or "WEU" if the contents are so marked.

68. Mark the envelope/package "Certified Official", this being endorsed by an authorising officer (see para 04099).

69. Insert the document and receipt (MOD Form 24) and seal the flap and seams of the envelope with security tape as described at Appendix 5.

70. If a Keepsafe security envelope is used seal in accordance with para 04073.

71. Packages - seal using wafer seals (see para 04078).

72. **Outer envelope/wrapping.** Select an unused envelope (or unused wrappings). Apply a legible stamp identifying the despatching organisation (eg. a branch stamp), and address to "HMS..., c/o BFPO 999". **No** protective marking is to appear on the envelope/package.

73. Insert inner envelope/package and seal the flap (or pack sticking down all seams).

74. Mark the envelope/package "Parcelforce 24" or "Defence mail service only" (if service available) in the top left-hand corner.

75. Despatch as described in para 76 below.

Normal Despatch

76. Sealed envelopes or packages should be placed in the "Out" tray for collection by transit services or forwarded to registries or Defence mail service collection points. In locations where several establishments are served by a single collection point, An audit trail will be required between the establishments and the collection point.

This page intentionally left blank

APPENDIX 3 TO ANNEX C TO CHAPTER 4

TRANSMISSION OF CONFIDENTIAL DOCUMENTS

SECTION I

TRANSMISSION WITHIN MOD OR SERVICE BUILDINGS/SITES OR BETWEEN APPROVED LOCATIONS (INCLUDING OTHER GOVERNMENT DEPARTMENTS) SERVED BY THE DEFENCE MAIL SERVICE (SEE PARA 3 OF ANNEX C)

WARNING

1. Envelopes or packages in transit must never be left unattended.

2. Mail to other Government departments in Central London not served by the Defence Mail Service (see para 3 of Annex C) should be despatched in accordance with Section III.

Preparation for Normal Despatch

1. Select one unused envelope (or unused wrappings), or an envelope of good quality to be used with an economy label, of suitable size and apply a legible stamp identifying the despatching organisation (eg. a branch stamp).

2. Address the envelope/package by name and/or appointment/branch plus room number and building/establishment. For locations outside central London, the address should include the appropriate town, eg. Royal Military Academy, Woolwich. The post code must not be included.

3. If the document bears a National caveat, eg. "UK EYES ONLY", the envelope is to be addressed "Exclusive to" and officer by name and appointment; the caveat must not appear on the envelope, etc.

4. The protective marking of contents **must not** be shown on the envelope, package. Descriptors, eg. "STAFF" may be shown.

5. Insert the document and seal the flap (or pack the document sticking down all seams).

6. Mark envelope "Defence mail service only".

Normal Despatch

7. Sealed envelopes or packages should be placed in the "out" tray for collection by transit services or forward to registries or mail collection points.

Despatch using Locked Pouches, etc

8. Documents transmitted in a locked pouch or box need not be enveloped unless the recipient is to forward them to a third party; the pouch, etc, is to be addressed to the intended recipient personally by name and/or appointment. (Key-holders are responsible for onward despatch (taking appropriate safeguards) of any documents received which are not of their concern). Pouches, etc should be conveyed by hand or despatched through normal transit services.

SECTION II

TRANSMISSION TO EMBASSIES AND HIGH COMMISSIONS IN CENTRAL LONDON SERVED BY THE DEFENCE MAIL SERVICE FROM APPROVED LOCATIONS ALSO SERVED BY THE DEFENCE MAIL SERVICE (SEE PARA 3 OF ANNEX C)

WARNING

1. Envelopes or packages in transit must never be left unattended.

Preparation for Normal Despatch

9. **Inner envelope/wrapping.** Select one unused envelope (or unused wrappings) of suitable size and apply a legible stamp identifying the despatching organisation (eg. a branch stamp) and the reference and date of origin of the document to be enclosed.

10. Address the envelope/package by name and/or appointment/branch plus room number and name of Embassy/High Commission. If the document bears a National caveat, eg. "UK/US EYES ONLY" the envelope/package is to be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope/package.

11. Mark "CONFIDENTIAL" boldly in red above and below the address; the protective marking should be prefixed "WEU" or "NATO" if the contents are so marked.

12. Insert the document and stick down the flap (or pack the document sticking down all seams).

13. **Outer envelope/wrapping.** Select a second unused envelope (or unused wrappings) and apply the address as at para 10 above. "PO Box 701, London WC2h 8BG" should be used as a return address; a branch stamp should **not** be used.

14. Insert the first envelope/package and stick down the flap (or pack sticking down all seams).

15. Mark envelope "Defence mail service only".

Note: The outer envelope/wrapping **must not** bear security markings.

Normal Despatch

16. Sealed envelopes or packages should be placed in the "out" tray for collection by transit services or forward to registries or mail collection points.

Despatch using Locked Pouches, etc

17. Documents transmitted in a locked pouch or box need not be enveloped unless the recipient is to forward them to a third party. The pouch is to be addressed to the intended recipient personally by name and/or appointment. (Key-holders are responsible for onward despatch (taking appropriate safeguards) of any documents received which are not of their concern). Pouches, etc should be conveyed by hand or despatched through normal transit services.

SECTION III

TRANSMISSION TO ADDRESSES IN THE UK OTHER THAN THOSE COVERED IN SECTION I & II OF APPENDIX 3 AND EXCLUDING NORTHERN IRELAND (SEE SECTION IV) FROM ANY MOD OR SERVICE LOCATION IN THE UK

WARNING

1. Parcels containing CONFIDENTIAL material must be prepared for despatch by Letter Post. Parcel post is not to be used.

2. CONFIDENTIAL documents are only to be sent to private addresses in exceptional circumstances and with specific permission from a head of establishment. They are not to be sent to addresses where foreign servants are employed or where there is no suitable container in which to keep them (see paras 04093 - 04094).

3. Envelopes or packages in transit must never be left unattended.

Preparation for Normal Despatch

18. **Inner envelope/wrapping.** Select one unused envelope (or unused wrappings) of suitable size and apply a legible stamp identifying the despatching organisation (eg. a branch stamp) and the reference and date of origin of the document to be enclosed.

19. Address the envelope/package by name and/or appointment/branch and full postal address.

20. If the document bears a National caveat, eg. "UK EYES ONLY", the envelope/package is to be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope/package.

21. Mark "CONFIDENTIAL" boldly in red above and below the address; the protective marking should be prefixed "WEU" or "NATO" if the contents are so marked.

22. Insert the document and stick down the flap (or pack the document sticking down all seams).

23. **Outer envelope/wrapping.** Select a second unused envelope (or unused wrappings).

24. For mail to official addresses, apply the address as at para 21 above.

25. For mail to private addresses, use a plain envelope; address by name without reference to rank, decorations, appointment, etc.

26. Mark the envelope/package "Letter Post" in the top left hand corner.

27. Insert the first envelope/package and stick down the flap (or pack sticking down all seams).

> ***Note*:** The outer envelope/wrapping **must not** bear security markings, branch stamp, or other marking which might associate it with the department. "PO Box 701, London WC2H 8BG" should be shown as the return address.

28. Mail for ships in UK ports or home waters should be addressed to "HMS..., c/o BFPO 999".

Normal Despatch

29. Sealed envelopes or packages, etc, should be placed in the "out" tray for collection by transit services or forward to registries or mail collection points.

SECTION IV

TRANSMISSION TO DIPLOMATIC POSTS ABROAD, AND OTHER ADDRESSES OVERSEAS INCLUDING NORTHERN IRELAND FROM ANY MOD OR SERVICE LOCATION IN THE UK

WARNING

1. In no circumstances may Post Office services be used for transmission of CONFIDENTIAL material to Northern Ireland or to other overseas locations.

2. Envelopes or packages in transit must never be left unattended.

3. CONFIDENTIAL material for foreign or Commonwealth Governments or their defence contractors may only be transmitted to those countries approved by the RMIPC and then only via the appropriate British Diplomatic Post.

4. Approval must be obtained from InfoSy(Industry)1/Command HQs before CONFIDENTIAL mail is sent (via the appropriate British Diplomatic post) to a foreign or Commonwealth-based defence contractor.

5. The appropriate MOD Form 189 (Condition of Release Stamp) must be firmly attached to each CONFIDENTIAL document sent to a foreign or Commonwealth Government, or defence contractor of that country. The prefix "UK" or where appropriate, "NATO" or "WEU" should appear before the protective marking on the document.

Preparation for Normal Despatch

30. Prepare and affix a completed despatch note (see Appendix 6) to documents intended for transmission to foreign or Commonwealth Governments or their defence contractors.

***Note*:** (1) For the transmission of mail to foreign or Commonwealth Governments or their defence contractors (sent via the appropriate British Diplomatic Post), see para 38.

(2) For the transmission of mail to British Defence Attaches/Advisers and to addresses in Northern Ireland, see para 31.

(3) For the transmission of mail to British officers or civilians serving in international organisations, see para 51.

(4) For the transmission of mail to HM Ships in overseas ports or waters, see para 58.

Mail to British Defence Attaches/Advisers and BFPO addresses including Northern Ireland

31. **Inner envelope/wrapping.** Select one unused envelope (or unused wrappings) of a suitable size. Apply a legible branch stamp identifying the despatching organisation (eg. a branch stamp) and the reference and date of origin of the document to be enclosed.

32. Address the envelope/package to the British Defence Attache/Adviser by name or appointment, with full address of the diplomatic post. For mail to Northern Ireland, address as appropriate.

33. If the document bears a (composite) National caveat, eg. "UK/US EYES ONLY", the envelope/package is to be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope/package.

34. Mark "CONFIDENTIAL" boldly in red above and below the address; the protective marking should be prefixed "UK", "NATO" or "WEU" if the contents are so marked.

35. Mark the envelope/package "Certified Official", this being endorsed by an authorising officer (see para 04100).

36. Insert document and seal flap (or pack sticking down all seams).

37. **Outer envelope/wrapping:**

a. For mail emanating from approved locations served by the Defence mail service (see para 3 of Annex C):

(1) Select an unused envelope (or unused wrappings).

(2) Apply a legible stamp identifying the despatching organisation (eg. a branch stamp), and address to "LCT, BFPO 1000". No protective marking is to appear on the envelope/package.

(3) Insert inner envelope/package and seal the flap (or pack sticking down all seams).

b. For mail emanating from other locations:

(1) Select an unused envelope (or unused wrappings.)

(2) Apply a legible stamp identifying the despatching organisation (eg a branch stamp), and address to "LCT, BFPO 1000". No protective marking is to appear on the envelope/package.

(3) Insert inner envelope/package and seal the flap (or pack sticking down all seams).

(4) Mark packages/letters "Letter Post".

(5) Despatch as described in para 65 below.

Mail to Foreign or Commonwealth Governments or their Defence Contractors (sent via the appropriate British Diplomatic Post)

38. **First envelope/wrapping.** Select one unused envelope (or unused wrappings) of a suitable size.

39. Address the envelope/package by name and/or appointment/branch and full postal address of the foreign or Commonwealth Government. Apply the reference and date of origin of the document to be enclosed.

40. If the document bears a (composite) National caveat, eg. "UK/US EYES ONLY", the envelope/package is to be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope/package.

41. Mark "CONFIDENTIAL" boldly in red above and below the address; the protective marking should be prefixed "UK", "NATO" or "WEU" if the contents are so marked.

42. Insert document and despatch note (see Appendix 6). Do **not** seal the flap or the envelope; packages should be loosely secured, ie. do not stick down seams.

43. **Second envelope/wrapping.** Select one unused envelope (or unused wrappings) of a suitable size. Apply a legible branch stamp identifying the despatching organisation (eg. a branch stamp) and the reference and date of origin of the document to be enclosed.

44. Address the envelope/package to the British Defence Attache/Adviser by name or appointment, with full address of the Diplomatic post.

45. If the document bears a (composite) National caveat, eg. "UK/US EYES ONLY", the envelope/package is to be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope/package.

46. Mark "CONFIDENTIAL" boldly in red above and below the address; the protective marking should be prefixed "UK", "NATO" or "WEU" if the contents are so marked.

47. Mark the envelope/package "Certified Official", this being endorsed by an authorising officer (see para 04099).

48. Insert first unsealed envelope/loosely secured package.

49. Seal flap (or pack sticking down all seams).

50. **Third (outer) envelope/wrapping:**

a. For mail emanating from approved locations served by the Defence mail service (see para 3 of Annex C):

(1) Select an unused envelope (or unused wrappings).

(2) Apply a legible stamp identifying the despatching organisation (eg a branch stamp), and address to "LCT, BFPO 1000". No protective marking is to appear on the envelope/package.

(3) Insert second envelope/package and seal the flap (or pack sticking down all seams).

(4) Despatch as described in para 65 below.

b. For mail emanating from other locations:

(1) Select an unused envelope (or unused wrappings).

(2) Apply a legible stamp identifying the despatching organisation (eg a branch stamp), and address to "LCT, BFPO 1000". No protective marking is to appear on the envelope/package.

(3) Insert second envelope/package and seal the flap (or pack sticking down all seams).

(4) Mark packages/letters "Letter Post".

(5) Despatch as described in para 65 below.

Mail to British Service Personnel or Civilians serving in International Organisations

51. **Inner envelope/wrapping.** Select one unused envelope (or unused wrappings) of a suitable size. Apply a legible branch stamp identifying the despatching organisation (eg. a branch stamp) and the reference and date of origin of the document to be enclosed.

52. Address the envelope/package by name and appointment with postal address (as appropriate) as follows:

Within SHAPE	-	c/o UKNMR SHAPE,BFPO 26
Within NATO (Brussels area)	-	c/o UK Delegation to NATO, Brussels, BFPO 49

Within SACLANT	-	c/o UKNLR to SACLANT, HMS SAKER, BFPO 2
Within WEU	-	c/o British Embassy, Paris

53. If the document bears a (composite) National caveat, eg. "UK/US EYES ONLY", the envelope/package is to be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope/package.

54. Mark "CONFIDENTIAL" boldly in red above and below the address; the protective marking should be prefixed "UK", "NATO" or "WEU" if the contents are so marked.

55. Mark the envelope/package "Certified Official", this being endorsed by an authorising officer (see para 04099).

56. Insert document and seal flap (or pack sticking down all seams).

57. **Outer envelope/wrapping.**

a. For mail emanating from approved locations served by the Defence mail service (see para 3 of Annex C):

(1) Select an unused envelope (or unused wrappings).

(2) Apply a legible stamp identifying the despatching organisation (eg a branch stamp), and address to "LCT, BFPO 1000". No protective marking is to appear on the envelope/package.

(3) Insert inner envelope/package and seal the flap (or pack sticking down all seams).

(4) Despatch as described in para 65 below.

b. For mail emanating from other locations:

(1) Select an unused envelope (or unused wrappings.)

(2) Apply a legible stamp identifying the despatching organisation (eg a branch stamp), and address to "LCT, BFPO 1000". No protective marking is to appear on the envelope/package.

(3) Insert inner envelope/package and seal the flap (or pack sticking down all seams).

(4) Mark packages/letters "Letter Post".

(5) Despatch as described in para 65 below.

Mail to HM Ships in Overseas Ports or Waters

58. **Inner envelope/wrapping.** Select one unused envelope (or unused wrappings) of a suitable size. Apply a legible branch stamp identifying the despatching organisation (eg. a branch stamp) and the reference and date of origin of the document to be enclosed.

59. Address the envelope/package by name and/or appointment to "HMS.....".

60. If the document bears a (composite) National caveat, eg. "UK/US EYES ONLY", the envelope/package is to be addressed "Exclusive to" an officer by name and appointment; the caveat must not appear on the envelope/package.

61. Mark "CONFIDENTIAL" boldly in red above and below the address; the protective marking should be prefixed "UK", "NATO" or "WEU" if the contents are so marked.

62. Mark the envelope/package "Certified Official", this being endorsed by an authorising officer (see para 04099).

63. Insert document and seal flap (or pack sticking down all seams).

64. **Outer envelope/wrapping:**

a. For mail emanating from approved locations served by the Defence mail service (see para 3 of Annex C):

(1) Select an unused envelope (or unused wrappings).

(2) Apply a legible stamp identifying the despatching organisation (eg a branch stamp), and address to "HMS ...., c/o BFPO 999". No protective marking is to appear on the envelope/package.

(3) Insert inner envelope/package and seal the flap (or pack sticking down all seams).

(4) Despatch as described in para 65 below.

b. For mail emanating from other locations:

(1) Select an unused envelope (or unused wrappings).

(2) Apply a legible stamp identifying the despatching organisation (eg a branch stamp) and address to "HMS...., c/o BFPO 999". No protective marking is to appear on the envelope/package.

(3) Insert inner envelope/package and seal the flap (or pack sticking down all seams).

(4) Mark packages/letters "Letter Post".

(5) Despatch as described in para 65 below.

Normal Despatch

65. Sealed envelopes or packages should be placed in the out tray for collection by transit services or forward to registries or mail collection points.

This page intentionally left blank.

APPENDIX 4 TO
ANNEX C TO
CHAPTER 4

TRANSMISSION OF RESTRICTED DOCUMENTS

SECTION I

TRANSMISSION WITHIN MOD OR SERVICE BUILDINGS/SITES OR BETWEEN APPROVED LOCATIONS (INCLUDING OTHER GOVERNMENT DEPARTMENTS) SERVED BY THE DEFENCE MAIL SERVICE (SEE PARA 3 OF ANNEX C)

WARNING

Envelopes or packages in transit must never be left unattended.

Preparation for Normal Despatch

1. Select one unused envelope (or unused wrappings), or an envelope of good quality to be used with an economy label, of suitable size, and apply a legible stamp identifying the despatching organisation (eg. a branch stamp). A transit envelope should not be used.

2. Address the envelope/package by name or appointment/branch plus room number and building/establishment. For locations outside central London, the address should include the appropriate town, eg. Royal Military Academy, Woolwich. The post code must not be included.

3. The protective marking (RESTRICTED) **must not** appear on the envelope/package; descriptors, eg. "STAFF" may be shown. (Alternatively, the term "to be opened by addressee only" may be used).

4. Insert the document and stick down the flap (or pack the document sticking down all seams).

5. Mark the envelope "Defence mail service only".

6. **Method of despatch.** Place in "out" tray for collection by transit services or forward to registries or mail collection points.

SECTION II

TRANSMISSION TO EMBASSIES AND HIGH COMMISSIONS IN CENTRAL LONDON SERVED BY THE DEFENCE MAIL SERVICE (SEE PARA 3 OF ANNEX C) FROM APPROVED LOCATIONS ALSO SERVED BY THE DEFENCE MAIL SERVICE

WARNING

Envelopes or packages in transit must never be left unattended.

Preparation for Normal Despatch

7. Select one unused envelope (or unused wrappings), or an envelope of good quality to be used with an economy label, of suitable size, and apply a legible stamp identifying the despatching organisation (eg. a branch stamp). A transit envelope should not be used.

8. Address the envelope/package by name and or appointment/branch plus room number and building/establishment.

9. The protective marking (RESTRICTED) **must not** appear on the envelope/package.

10. Insert the document and stick down the flap (or pack the document sticking down all seams).

11. Mark the envelope "Defence mail service only".

12. Method of despatch. Place in "out" tray for collection by transit services or forward to registries or mail collection points.

SECTION III

TRANSMISSION TO ADDRESSES IN THE UK OTHER THAN THOSE COVERED IN SECTION I & II OF APPENDIX 4 EXCLUDING NORTHERN IRELAND (SEE SECTION IV) FROM ANY MOD OR SERVICE LOCATION IN THE UK

WARNING

Envelopes or packages in transit must never be left unattended.

Preparation for Normal Despatch

13. Select one unused envelope (or unused wrappings), or an envelope of good quality to be used with an economy label, of suitable size. A transit envelope should not be used.

14. For mail to private addresses, use a plain envelope; address by name without reference to rank, decorations, appointments, etc.

15. Mail to and from locations **not** served by the Defence mail service should be given the full postal address.

16. The protective marking (RESTRICTED) **must not** appear on the envelope/package; where descriptors are used, the envelope must be marked "To be opened by addressee only".

17. The envelope/wrapping must not bear any markings, branch stamp, etc, which might associate it with the department. "PO Box 701 London WC2 8BG" should be shown as the return address.

18. Insert the document and stick down the flap (or pack the document sticking down all seams).

19. **Method of despatch.** Place in "out" tray for collection by transit services or forward to registries or mail collection points.

SECTION IV

TRANSMISSION TO DIPLOMATIC POSTS ABROAD AND OTHER ADDRESSES OVERSEAS, INCLUDING NORTHERN IRELAND, FROM ANY MOD OR SERVICE LOCATION IN THE UK

WARNING

1. Envelopes or packages in transit must never be left unattended.

2. RESTRICTED (and UNCLASSIFIED) mail to Northern Ireland should be addressed to the appropriate establishment by BFPO number. Mail should only be sent to private addresses in Northern Ireland or the Republic of Ireland in exceptional circumstances (see para 04096). RESTRICTED mail to other private addresses is only to be despatched in accordance with para 04106.

3. RESTRICTED material for foreign or Commonwealth Governments or their defence contractors may only be transmitted to those countries approved by the RMIPC. RESTRICTED material to such organisations in countries listed in para 6 of Annex C and para 23 below, must be sent via the appropriate British diplomatic post.

4. Approval must be obtained from InfoSy(Industry)1 before RESTRICTED mail is sent to any defence contractor in the countries listed in para 23 below.

5. The appropriate MOD F 189 (Condition of Release Stamp) must be firmly attached to each RESTRICTED document sent to a foreign or Commonwealth Government or defence contractor of that country. The prefix UK or, where appropriate, NATO or WEU should appear before the protective marking on the document.

Preparation for Despatch

20. These instructions apply to both RESTRICTED and UNCLASSIFIED documents.

21. Private addresses. Mail for private addresses should be sent in accordance with the appropriate advice contained in either paras 04096 or 04106.

22. Ships. Mail for ships in overseas ports or waters should be addressed to "HMS..., BFPO..." (see para 04107). A legible branch stamp incorporating the **full** postal address of the sender may be used to indicate the return address. Where this is not possible the return address should be "PO Box 701 London WC2H 8BG".

23. Companies in America/Australia/Austria/Canada /Israel/Italy/ Netherlands/ Republic of Korea/Spain and Switzerland. Mail addressed to any companies based in America, Australia, Austria, Canada, Israel, Italy, Netherlands, Republic of Korea, Spain or Switzerland must be prepared as follows:

a. **Inner envelope/wrapping.**

(1) Select one unused envelope (or unused wrappings) of suitable size and apply the reference and date of origin of the document to be enclosed. "PO Box 701 London WC2H 8BG" should be used as a return address; a branch stamp is **not** required.

(2) Address the envelope/package to the company concerned by name and full address.

(3) Mark "UK RESTRICTED" boldly in red above and below the address.

(4) Insert the document and stick down the flap (or pack the document sticking down the seams).

b. **Outer envelope/wrapping - for companies in Australia, Austria, Israel, Netherlands, Republic of Korea, Spain and Switzerland.**

(1) Prepare a second unused envelope (or wrappings), applying details as at 23a(1) above. Insert the first envelope/package (together with a completed Despatch Note (see Appendix 6) and stick down the flap (or pack sticking down all seams); address the second envelope/package, as appropriate, to:

(a) Defence Advisor
British High Commission
Commonwealth Avenue
Yarralumla, Canberra, ACT 2600 Australia

or

(b) Defence Attaché
British Embassy
Jauresgasse 12
1030 Vienna, Austria

or

(c) Defence Attaché
British Embassy
192 Hayarkon Street
Tel Aviv 63404, Israel

or

(d) Defence Attaché
British Embassy
Lange Voorhout
102514 ED
The Hague
Netherlands

or

(e) Defence Attaché
British Embassy
4 Chung-Dong
Chung-Ku
Seoul
Republic of Korea

or

(f) Defence Attaché
British Embassy
Calle de Fernanado el Santo 16
Madrid 4
Spain

or

(g) Defence Attaché
British Embassy
Thunstrasse 50
3005 Berne
Switzerland

c. **Outer envelope - for companies in America, Canada and Italy.** The full company name and address as detailed on the inner envelope in accordance with sub-paragraph 23a(2) above. Receipts (MOD F24) are required.

24. Use of the diplomatic bag. Mail addressed to diplomatic posts in countries listed at para 6 of Annex C must always be despatched by diplomatic bag. The following procedure should be followed:

a. **Inner envelope/wrapping.**

(1) Select one unused envelope (or unused wrappings) of suitable size and apply a legible stamp identifying the despatching organisation (eg a branch stamp) and the reference and date of origin of the document to be enclosed.

(2) Address the envelope by name and/or appointment and branch with full postal address.

(3) Mark "RESTRICTED" or "UNCLASSIFIED" boldly in red above and below the address.

(4) Insert the document (together with a completed Despatch Note (see Appendix 6) where the document is intended for onward transmission to a foreign or Commonwealth Government or its defence contractor) and stick down the flap (or pack the document sticking down all seams).

(5) Mark the envelope/package "Certified Official", this being endorsed by an authorizing officer (see para 04101).

b. **Outer envelope/wrapping.** Select a second unused envelope (or unused wrappings) and address to HQ DCS, BFPO 747. A legible branch stamp incorporating the **full** postal address of the sender may be used to show the return address. Where this is not possible, the return address given should be "PO Box 701 London WC2H 8BG". Insert the first envelope/package and stick down the flap (or pack sticking down all seams).

25. Other destinations. For destinations other than those shown at para 23b above, select one unused envelope (or unused wrappings), or an envelope of good quality to be used with an economy label, of suitable size and apply the reference and date of origin of the document to be enclosed. In the case of UNCLASSIFIED mail, the reference and date of origin of the document enclosed may be omitted from the envelope. Address the envelope/package by name and/or appointment/branch and full postal address. "PO Box 701 London WC2H 8BG" should be used as a return address; a branch stamp is **not** required. The protective marking (RESTRICTED) **must not** appear on the envelope/package.

26. Method of despatch. Place in "out" tray for collection by transit services or forward to registries or mail collection points.

This page intentionally left blank

APPENDIX 5 TO

ANNEX C

SEALING OF ENVELOPES WITH HIGH SECURITY TAPE

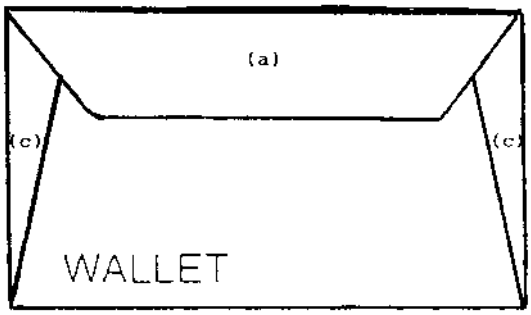
1. High security tape must be applied over all the envelope's seams, avoiding the need for small pieces of tape; pocket or wallet style envelopes should be used, seam arrangements simplifying tape application. **Pocket** style envelopes have a straight sealing flap on one narrow side with a sealed flap opposite, and a seam running the length of the envelope. **Wallet** style envelopes have a straight edge sealing flap along their length, and side seams. **Banker** style envelopes are **not** suitable for use with the tape; These have a triangular shaped sealing flap situated on one broad side of the envelope and seams running diagonally across the envelope.

2. Moisten and stick down the gummed flap of the envelope. Apply high security tape to cover the flap edge; tape should extend at least 1.5 cm on to the front of the envelope. On pocket style envelopes, then apply tape to the sealed flap opposite. Tape remaining seam(s) on the envelope last, overlapping tape on to other flaps/seams and extending beyond crossover points on to the front of the envelope so that both ends of each piece of tape are visible and seen to be firmly stuck to the envelopes surface. Tape should always be applied to flaps/seams **parallel** to the nearest edge of the envelope. See diagrams below.

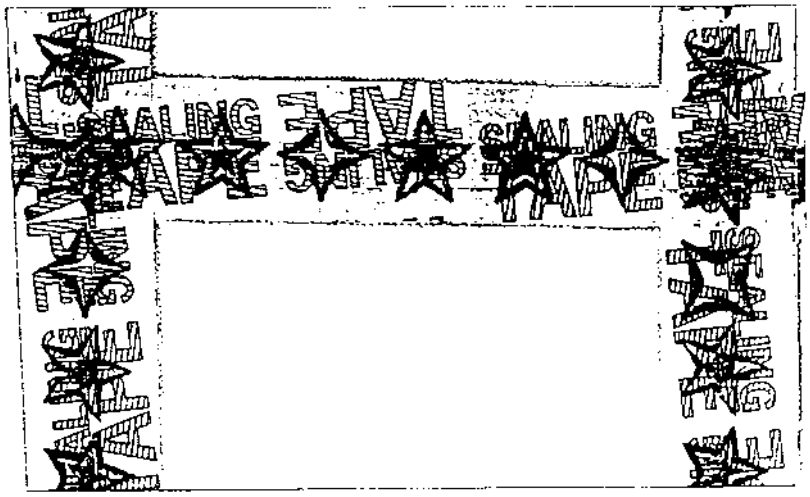
> ***Note:*** Some envelopes have deep flaps/seams which cannot be completely covered by single widths of high security tape. In such cases additional strips of tape should be applied to cover the exposed joins and extending round to the front of the envelope as described above.

3. Care should be taken to ensure address labels, where used, do not prevent application of the tape directly to the surface of the envelope. Similarly, address labels should not be applied so that they obscure high security tape.

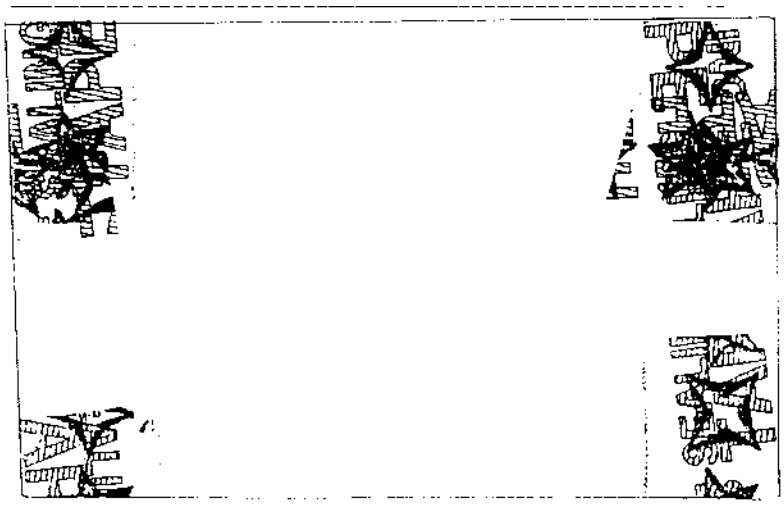
Wallet style envelope



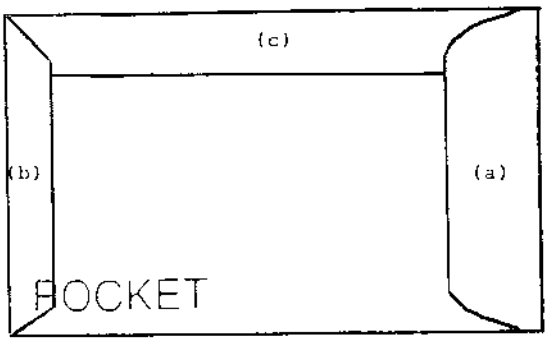
Wallet style envelope sealed - back



Wallet style envelope sealed - front

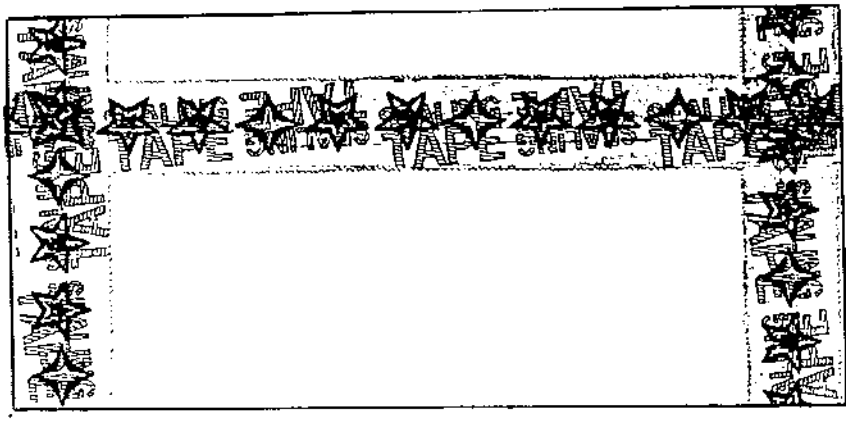


Pocket style envelope

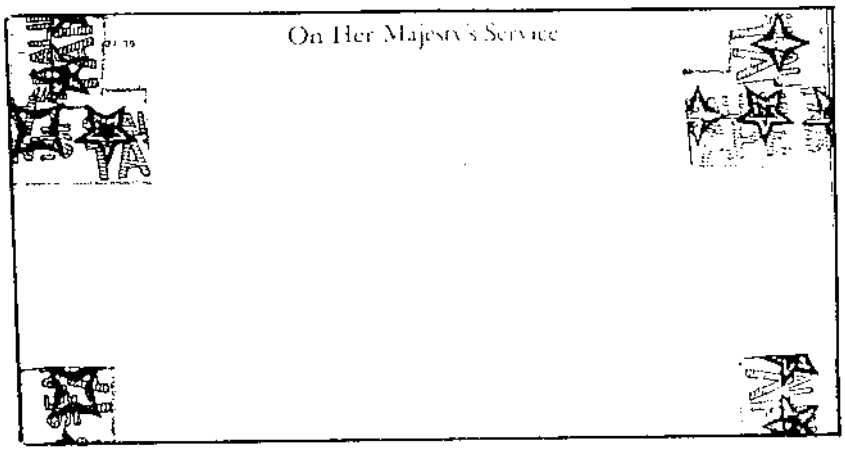


Pocket style envelope sealed - back

Flap B

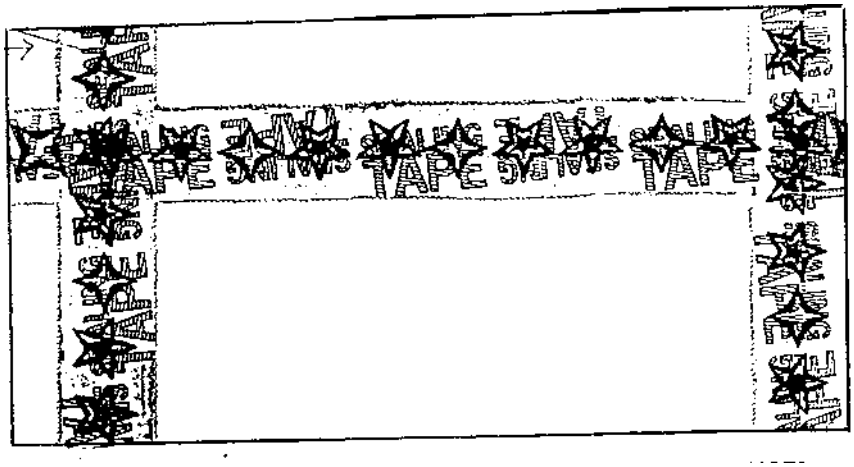


Pocket style envelope sealed - front



Pocket style envelope with deep flap back incorrectly sealed

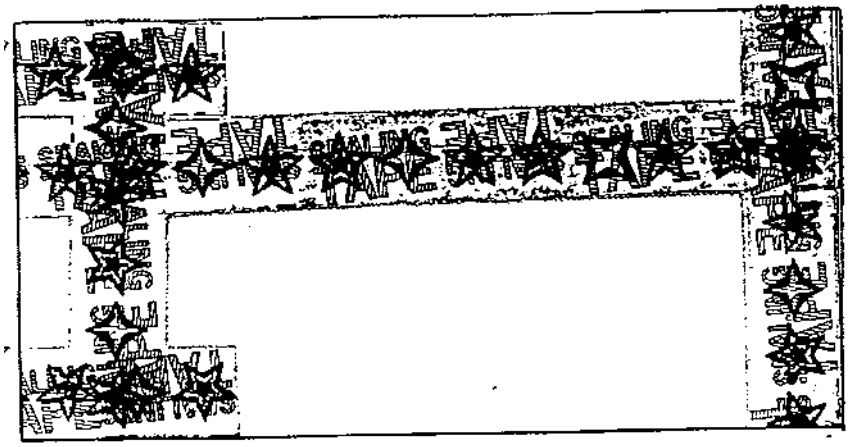
Deep flap not completely covered by tape



Pocket style envelope - back correctly sealed

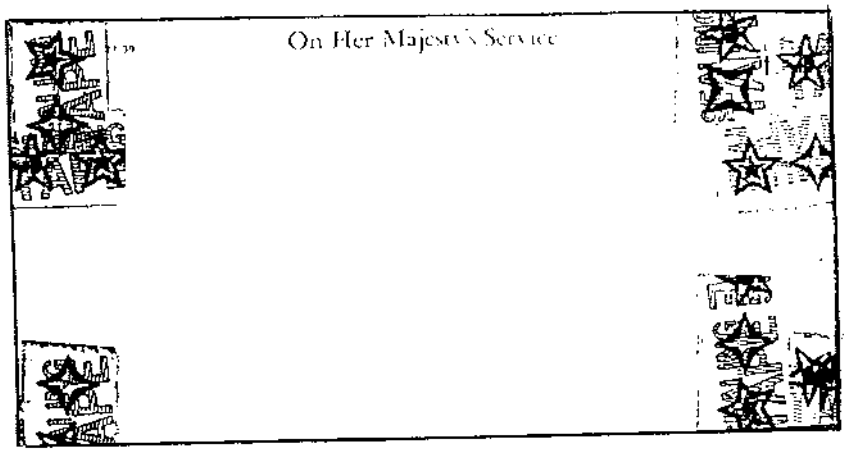
Extra strip of sealing tape

Extra strip of sealing tape



Pocket style envelope - front view correctly sealed

Extra strips of tape extending to front of envelope



APPENDIX 6 TO
ANNEX C TO
CHAPTER 4

SPECIMEN DESPATCH NOTE

UNCLASSIFIED covering (insert protective marking)

To: (British Defence Attache/Advisor) From:

_____ _____

_____ _____

_____ _____

Date:

Reference:

The documents listed below have been approved by the Ministry of Defence for release to (insert full postal address of government or contractor facility)

_____

_____

_____

(Insert details of enclosed documents)

Reference No Protective Marking Date

_____

_____

_____

Would you please arrange for their onward transmission through the appropriate security channel.

Signed_____

UNCLASSIFIED covering (insert protective marking)

This page intentionally left blank

APPENDIX 7 TO ANNEX C TO CHAPTER 4

TRANSMISSION OF DOCUMENTS BEARING DESCRIPTORS AND RESTRICTIVE MARKINGS

Rules on the transmission of such material are produced below for the convenience of despatch staff.

Documents bearing descriptors	CONTROLLED DISTRIBUTION REQUIRED Material
In accordance with that for relevant protective markings. For transmission outside MOD van service locations, double envelope. Protective marking/descriptor to be shown on inner envelope. For transmission with MOD van service/hand delivery, single envelope. Descriptor only may be shown on the envelope.	Address : by name or appointment a. Despatch to : MOD buildings or via Defence mail service Enveloping : Single Marking : Single envelope to be marked "Personal" together with the legend "To be opened only by (named addressee)" b. Despatch to : Elsewhere in UK Enveloping : Double Marking : Inner envelope to be marked as for a. c. Despatch to : Overseas Envelope and despatch in accordance with regulations as detailed in Section IV, Appendix 2, Chapter 4. Notes: (1) In all the above cases the restrictive marking "CONTROLLED DISTRIBUTION REQUIRED" should not appear on inner, single or outer envelopes. (2) MOD Form 24 receipts are mandatory for all despatches except within a MOD HQ building.

This page intentionally left blank

METHODS OF TRANSMISSION WITHIN AND FROM UK – SUMMARY

Protective marking	Destination	Type of covering and marking (if required)	Sealing	Receipt	Transmission
TOP SECRET	Any addressee	Single wrapping + appropriate marking(s) + MOD Form 488 **or** Keepsafe envelope + MOD Form 488	security tape Stick down flap	Yes	By hand of courier. For diplomatic posts abroad include "c/o LCT BFPO 1000". For ships in UK or overseas include "c/o BFPO 999"
SECRET	1. Within MOD bldgs or between approved locations (inc OGDs) served by the Defence Mail Service	Single wrapping – no protective marking **or** Pouch (see Note 1)	Stick down flap	Yes – outside the building	Defence Mail Service
SECRET	2. Embassies and High Commissions in Central London served by the Defence Mail Service	Double wrapping + appropriate marking(s) on the inner wrapping only **or** Pouch (see Note 1)	Stick down flap	Yes	Defence Mail Service
SECRET	3. Addresses in UK other than 1 and 2 above (excluding NI)	Double wrapping + appropriate marking(s) on the inner wrapping only	Stick down flap	Yes	1. Parcelforce 24 2. Parcelforce 10 and 12 (see Note 2) 3. Special Delivery Service

Protective marking	Destination	Type of covering and marking (if required)	Sealing	Receipt	Transmission
SECRET	4. Overseas including NI a. Foreign and Commonwealth Govts or their defence contractors	See Annex C Appendix 2, Section IV for detailed instructions Triple wrapping + appropriate marking(s) on the 1st and 2nd inner wrappings but not the outer wrapping.	1st wrapping should NOT be sealed 2nd wrapping to be sealed with security tape or use Keepsafe envelope 3rd wrapping to be stuck down	Yes	1st. Address to the foreign govt or company 2nd. Address to the responsible British Embassy official 3rd. Address to LCT BFPO 1000 and use approved mail services.
SECRET	b. Defence Attachēs/ Advisers and NI	Double wrapping + appropriate marking(s) on the inner wrapping only	1st wrapping seal with security tape or use Keepsafe envelope 2nd wrapping to be stuck down	Yes	1st. Address to the Defence Attache/ Adviser or official address in NI. 2nd. Address to LCT BFPO 1000 and use approved mail services.

Protective marking	Destination	Type of covering and marking (if required)	Sealing	Receipt	Transmission
SECRET	c. British officers/ civilians serving in international organisations	Double wrapping + appropriate marking(s) on the inner wrapping only	1st wrapping to be sealed with security tape or use Keepsafe envelope 2nd wrapping to be stuck down (see note 3)	Yes	1st. Address to person concerned and the appropriate international organisation. 2nd. Address to LCT BFPO 1000 and use approved mail services.
SECRET	d. HM Ships in overseas ports or waters	Double wrapping + appropriate marking(s) on the inner wrapping only	1st wrapping to be sealed with security tape or use Keepsafe envelope 2nd wrapping to be stuck down	Yes	1st. Address to appropriate person or CO of the ship using appropriate BFPO number. 2nd. Address c/o BFPO 999 using approved mail services.
CONFIDENTIAL	1. Within MOD bldgs or between approved locations (inc OGDs) served by Defence Mail Service	Single wrapping with no protective marking showing **or** Pouch (see Note 1)	Stick down flap	No	Defence Mail Service

Protective marking	Destination	Type of covering and marking (if required)	Sealing	Receipt	Transmission
CONFIDENTIAL	2. Embassies and High Commissions in Central London served by the Defence Mail Service	Double wrapping + appropriate marking(s) on the inner wrapping only **or** Pouch (see Note 1)	Stick down flaps	No	Defence Mail Service
CONFIDENTIAL	3. Addresses in the UK other than 1 and 2 above (excluding NI)	Double wrapping + appropriate marking(s) on the inner wrapping only	Stick down flaps	No	2nd Class letter post. For Ships in home ports or waters address c/o BFPO 999
CONFIDENTIAL	4. Overseas including NI a. Foreign or Commonwealth Govts or their defence contractors	See Annex C Appendix 3, Section IV for detailed instructions Triple wrapping + appropriate marking(s) on the 1st and 2nd inner wrappings but not the 3rd outer one	1st wrapping should NOT be sealed 2nd wrapping to be stuck down 3rd wrapping to be stuck down	No	1st. Address to the foreign govt or company. 2nd. Address to the responsible British Embassy official. 3rd. Address to LCT BFPO 1000 and use approved mail services.

Protective marking	Destination	Type of covering and marking (if required)	Sealing	Receipt	Transmission
CONFIDENTIAL	b. Defence Attachēs/ Advisers and NI	Double wrapping + appropriate marking(s) on inner wrapping only	Stick down flap	No	1st. Address to the Defence Attache/ Adviser or official address in NI. 2nd. Address outer envelope to LCT BFPO 1000 and use approved mail services.
CONFIDENTIAL	c. British officers/ civilians serving in international organisations	Double wrapping + appropriate marking(s) on inner wrapping only	Stick down flap	No	1st. Address to person concerned at the appropriate international organisation. 2nd. Address outer envelope to LCT BFPO 1000 and use approved mail services.
CONFIDENTIAL	d. HM Ships in overseas ports or waters	Double wrapping + appropriate marking(s) on inner wrapping only	Stick down flap	No	1st. Address to appropriate person or CO of the ship using appropriate BFPO number. 2nd. Address c/o BFPO 999 using approved mail services.

Protective marking	Destination	Type of covering and marking (if required)	Sealing	Receipt	Transmission
RESTRICTED	1. Within MOD bldgs or between approved locations (inc OGDs) served by Defence Mail Service	Single wrapping with no protective marking showing	Stick down flap	No	Defence Mail Service
RESTRICTED	2. Embassies and High Commissions in Central London served by the Defence Mail Service	Single wrapping with no protective marking showing	Stick down flap	No	Defence Mail Service
RESTRICTED	3. Addresses in the UK other than 1 and 2 above (excluding NI)	Single wrapping with no protective marking showing	Stick down flap	No	2nd Class letter post
RESTRICTED	4. Overseas including NI	Double wrapping + appropriate marking(s) on the inner wrapping only	Stick down flaps	No (see Note 4)	British Forces Post Office or letter post. For mail to diplomatic posts in countries listed at para 6 of Annex C the outer wrapping should be addressed "HQ DCS BFPO 747"

Note: 1. Documents transmitted in a locked pouch or box need not be enveloped unless the recipient is to forward them to a third person.
2. The use of Parcelforce 10 and 12 is more expensive than Parcelforce 24. D Def PCS agreement should be obtained for their use.
3. For mail emanating from locations not served by the British Forces Post Office the outer wrapping should be marked "Parcelforce 24" in the top left hand corner.
4. Receipts are required for RESTRICTED documents transmitted to America, Canada and Italy.

ANNEX E TO CHAPTER 4

SPECIMEN FORM OF APPLICATION FOR AUTHORITY TO TAKE DOCUMENTS MARKED CONFIDENTIAL OR ABOVE OVERSEAS

To (Insert appropriate Principal Security Adviser)

1. Authority is requested for the personal carriage of protectively marked documents overseas by casual courier.

2. Personal details of proposed courier:

a. Surname_____

Forenames_____

b. Rank/grade_____ c. Establishment_____

d. Tel No_____ e. Building/Room No_____

Passport details:

f. Passport No_____ g. Place of Issue_____

h. Date_____ i. Date of last renewal_____

3. Details of document(s) to be carried (ref. No. of document with highest protective marking to be given):

a. Protective marking_____ b. Ref. No._____

c. Indicate:

(1) If NATO documents_____ (2) If UK documents_____

(3) If other documents (describe)_____

d. Reasons why personal carriage is necessary_____

_____

_____

4. Itinerary of journey:

a. Countries to be visited (also destinations within countries visited)

_____
_____

b. Method of travel (if by air, state whether RAF or civil; if civil state flight no. and airline).

Date of Journey	**From (airport/port of departure)**	**To (airport/port of arrival**

5. State reasons why documents cannot be sent in advance by Defence Courier Service or FCO Queens Messenger.

_____
_____
_____

Note: Casual courier status affords reduced protection for protectively marked documents in transit and will only be authorized when absolutely necessary.

_____

Head of Establishment

Name(block capitals)_____

Rank/grade_____

Date_____

Branch Stamp

ANNEX F TO
CHAPTER 4

MINISTRY OF DEFENCE

CASUAL COURIER AUTHORIZATION CERTIFICATE

Reference No._____

This is to certify that_____

Holder of passport no. _____, an official of the United Kingdom Government is authorised to carry on the journeys detailed below package(s) containing official documents relating to the work carried out by the Ministry of Defence in the interests of the United Kingdom Government/North Atlantic Treaty Organisation, and bearing reference no. _____ together with the stamp and signature which appears at the foot of this authorization; and that the contents consist solely of documents.

Itinerary

	Outward	**Return**
Date		
Method of Travel		
From		
To		

Date of Issue

Stamp of authorizing official,
or establishment

Signature of directorate, division
authorizing official

Name_____
Rank/Grade_____

(**DUPLICATE**: To be held by the establishment security officer).

MINISTRY OF DEFENCE
CASUAL COURIER AUTHORIZATION CERTIFICATE

Reference No._____

This is to certify that_____

Holder of passport no. _____, an official of the United Kingdom Government is authorised to carry on the journeys detailed below package(s) containing official documents relating to the work carried out by the Ministry of Defence in the interests of the United Kingdom Government/North Atlantic Treaty Organisation, and bearing reference no. _____ together with the stamp and signature which appears at the foot of this authorization; and that the contents consist solely of documents.

Itinerary

	Outward	**Return**
Date		
Method of Travel		
From		
To		

Date of Issue

Stamp of authorizing official,
or establishment

Signature of directorate, division
authorizing official

Name_____
Rank/grade_____

(A certificate of undertaking must be completed by the casual courier prior to the journey).

ANNEX G TO CHAPTER 4

INSTRUCTIONS TO OFFICERS ON THE PERSONAL CARRIAGE OF PROTECTIVELY MARKED DOCUMENTS OVERSEAS

(To be issued with, but separately from, each Authorization)

1. These instructions are to be carefully observed.

2. The package is addressed to you care of _____(establishment to be visited).

3. You should ensure that a list of all documents that you will carry has been prepared in duplicate and that the original has been left with your directorate or establishment. The duplicate list must not be inside the package containing the documents.

4. You should carry the package in a brief case or similar container of a type detailed in sub para 04111b. Except in the circumstances described in para 9 below, you should not open the package until you reach your destination. You should ensure that during your journey the package does not leave your possession, thus you should not leave it in hotel rooms or deposit it in hotel safes, luggage offices or lockers. At your destination you should, wherever practicable, have the documents housed overnight with a United Kingdom overseas Government representative or an authority (see 7 below) approved by your Principal Security Adviser. If this is not practicable the documents must not leave your personal custody even for a moment.

5. While carrying these documents you are not to travel:

a. By air over, or by airline of, any of the following countries:

Afghanistan
Belarus
China (including Hong Kong SAR, Tibet and Macao)
Cuba
Iran
Iraq
Lebannon
Libya
North Korea
Russia
Sudan

Syria
Ukraine
Vietnam
Yugoslavia (Serbia and Montenegro)

b. By surface route to or through countries other than the following:

Australia	Japan*
Austria *	Netherlands
Belgium	New Zealand*
Canada	Norway
Denmark	Portugal
France	Spain
Germany	Sweden*
Greece	Switzerland*
Iceland	Turkey
Italy	United States

* Delete if NATO documents are being carried.

6. You are not to discuss the documents you are carrying in any public place.

7. Should you lose the documents or if you are unable, because of sickness or for any other reason, to safeguard them, you should seek immediate assistance from a British Embassy, High Commission or Consular Officer (or Diplomatic Mission or Government Department of any NATO country, NATO International Command or Agency).+

\+ If NATO documents are not being carried delete the words in brackets.

8. Wherever practicable you should return the documents to the United Kingdom by diplomatic bag through a British Embassy, High Commission or Consular Office. (The package should be open so that the contents can be verified in order to comply with regulations) but it may be sealed in the presence of the Embassy, High Commission or Consular Officer who receives it. If it is necessary for you to carry the documents back with you, you should place them in the spare cover provided bearing the same reference number, stamp and signature as used on the outward journey. The cover must be sealed with wafer seals. (Wafer seals should have the addition of a signature in ink across the seals and the package which should be reinforced by strips of cellulose tape covering the seals and seams. If you have no means of sealing the package in this way you should make the best use of whatever adhesive material is available.) You should address it to yourself at your department.

9. There is no assurance of immunity from search by customs, Airport or Port officials of the countries whose borders you will be crossing. If any official inquires into the contents of the package, you should show your authorization but not these instructions, which must be kept separate from the authorization. This may suffice to pass the package (but not necessarily the briefcase) through the customs unopened. If, nevertheless, an official demands to see the contents of the package you may open it but should take precaution to show him only as much of the contents as will satisfy him that the package contains nothing more than it purports to contain. On no account should you allow the package out of your possession or permit a full examination of the documents. You should request the official to provide evidence of the opening and inspection of the package, for example, by signing or stamping it when closed. You should reseal the package.

10. If you have been obliged to open the package at the request of an official of the country you are visiting, you should where possible notify the local British Embassy, High Commission or Consular Office and you should report the incident to your Principal Security Adviser or to your security officer on your return. If the action was taken by a United Kingdom official you should also inform the above authorities.

11. On your return you should personally verify with the officer holding the duplicate list that all documents have been returned or receipts obtained.

12. On your return you must send your authorization certificate to your security officer and notify him of any incident of possible security significance. For example, any failure or inability on your part to safeguard the documents or any undue interest on the part of other persons in what you were carrying.

This page intentionally left blank

ANNEX H TO CHAPTER 4

INSTRUCTIONS TO OFFICERS ON THE PERSONAL CARRIAGE OF PROTECTIVELY MARKED DOCUMENTS OVERSEAS

I certify that I have read and understood the above instructions and that I undertake to observe them.

Signature.....

Name in block letters.....

Rank .....

Establishment.....

Date.....

A list of documents has been left with:

(Name).....

This page intentionally left blank

ANNEX I TO CHAPTER 4

GUIDELINES TO COURIERS IN REGARD TO HIJACKING

(The following advice should be given to all couriers on the threat from hijacking and measures to be taken to counter this threat.)

1. There is an ever present threat of hijacking on all commercial routes worldwide.

2. British airlines are given official advice on security measures against hijacking. These airlines can therefore be relied on to a greater extent than others. These airlines or service aircraft or aircraft on charter to the Armed Services should be used whenever possible.

3. A casual courier should return from overseas with as few protectively marked documents as possible.

4. If a courier is involved in a hijack he/she should do nothing to draw attention to him/herself.

5. At the conclusion of a hijacking when passengers are freed, the courier should whenever possible carry away the documents.

6. If a courier is freed but is forced by hijackers to leave the documents on board the aircraft, he/she should, if possible, ascertain the destination of the aircraft from the airport authorities and have the UK mission or protecting power at the destination informed of the presence of the documents so that action can be taken to recover them.

This page intentionally left blank

ANNEX J TO CHAPTER 4

DESCRIPTORS

1. Descriptors may be helpful in implementing the "need to know" principle by indicating the nature of the asset's sensitivity and thereby helping to ensure that access is limited accordingly. Aside from PERSONAL, which by definition requires that the information is only made available in the first instance to the addressee, the descriptors will normally be used in conjunction with a protective marking. Used alone, descriptors may indicate who should see the material but do not of themselves impose any particular handling or level of protection. A list of MOD descriptors is below:

a. **APPOINTMENTS.** Concerning actual or potential appointments that have not been announced.

b. **BUDGET.** Concerning proposed or actual measures for the Budget before they are announced.

c. **COMMERCIAL.** Subject matter of actual or potential commercial value, the disclosure of which would prejudice a commercial interest. The rules for the use of this marking are given in Chapter 12.

d. **CONTRACTS.** Matters concerning tenders under consideration and the terms of tenders accepted.

e. **CONTROL (or DS).** Exercise papers for use only by control or directing staff. (For MOD use only.)

f. **EXAMINATION.** Subject matter relating to setting, marking or future examination papers. (For MOD use only.)

g. **EXERCISES.** Concerning orders and instructions pertaining to military exercises at home and abroad. (For MOD use only.)

h. **HONOURS.** Matters concerning military or civilian honours and awards.

i. **INTELLIGENCE.** Concerning intelligence source material and assessments. (For MOD use only.)

j. **INVESTIGATION.** Concerning investigations into disciplinary or criminal matters.

k. **LOCSEN.** Concerning locally sensitive information.

l. **MANAGEMENT.** Management policy and planning matters, the premature disclosure of which would not be in the interest of the Ministry of Defence or the Services.

m. **MEDICAL.** Medical matters concerning individuals including reports and records.

n. **OPERATIONS.** Concerning orders and instructions pertaining to military operations at home and abroad. (For MOD use only.)

o. **PERSONAL.** Material only to be seen by the person to whom it is addressed.

p. **POLICE.** Police matters concerning police operations and activities. (For MOD use only.)

q. **POLICY.** Concerning proposals for new or changed policy before publication.

r. **REGULATORY.** Material which has come into the possession of government departments or agencies in the course of carrying out their statutory regulatory duties.

s. **STAFF.** Matters concerning the administration (eg confidential reports), discipline, security status and service of named or identifiable personnel.

t. **VETTING.** Concerning matters pertaining to the security clearance of personnel. (For MOD use only.)

u. **VISITS.** Concerning details of visits by, for example, Royalty, ministers or very senior staff.

2. Should additions to this list be sought, they should be addressed to D Def Sy through the security reporting chain.

ANNEX K TO CHAPTER 4

CODEWORDS, NICKNAMES AND THE PROTECTION OF COMPARTMENTED INFORMATION

Codewords and nicknames

1. **Definitions.** A codeword is a single word that is always expressed in CAPITAL letters and is used to provide security cover for reference to a particular protected matter. A nickname is a name made up of two words selected by the originator and used for convenience for reference to any matter where security protection is not required.

2. It is important to understand the difference between codewords (which provide security cover) and nicknames (which do not) because confusion in the use of these terms could lead to breaches of security. The adoption of local or unofficial terms or procedures (eg `code names') is forbidden.

3. **Use of codewords.** Codewords are to be used solely for security purposes and only registered codewords may be used. The primary purpose of codewords is to conceal intentions, but they may also be used to limit the knowledge of particular matters. They may be used:

a. As names for protected plans, projects, equipments, etc.

b. To describe or initiate phases of operations.

c. To initiate action for emergency or contingency plans.

d. To provide a short reference to a protected matter, knowledge of which must be restricted to a limited circle of people.

e. To identify protected documents with a limited circulation, ie subject to special handling procedures.

4. **Control and Allotment of Codewords.** All codewords are to be taken from the United Kingdom Codeword Index maintained by the Defence Crisis Management Centre (DCMC). The DCMC makes block allocations of codewords to lead Commands; Service establishments are to apply for codewords or information about codewords to Command HQs. Blocks of codewords not yet taken into use should be treated as CONFIDENTIAL documents to avoid any risk of compromise in their subsequent use. Central Staffs branches should apply for codewords or information about codewords direct to DCMC. DPA and DLO staff should apply to

their Principal Security Adviser. In the event of a codeword being required out of normal working hours, application may be made to the Chief of the Defence Staff's Duty Officer.

5. **Notification of Use.** When a codeword is taken into use, its meaning, with the protective marking for both the codeword itself and its meaning, must be notified by the user to the issuing authority through normal channels. Any changes must be notified as they occur. Codewords taken into use but subsequently cancelled may not be re-used without authority from the issuing authority.

6. **Procedure for Bringing Codewords into Use.** The user of a codeword is responsible for allotting a meaning to it with protective markings for both the codeword itself and its meaning. The user should ensure, in conjunction with the issuing authority, that within the limitations of the available registered words, the codeword chosen is suitable for the matter to which it is to refer, namely, it should be:

a. Neither frivolous nor likely to invest the matter with an undesirable significance.

b. Unrelated to the meaning, eg ICEBERG is unsuitable for cold weather operations.

c. Unrelated to other words of a series, eg a series of bird names is unsuitable for, say, the various phases of an operation.

7. **The Meaning.** The meaning given to a codeword is to be specific and self-explanatory but should not reveal more than is necessary.

8. **Protective Marking.** The purpose of a codeword is to conceal the meaning attached to it and as long as this concealment is complete there is normally no reason for the codeword itself, as opposed to its meaning, to attract a protective marking. An unclassified codeword may be used in an unclassified letter or in a telephone conversation in clear to convey a protected meaning, eg contingency plans may have a high protective marking but the order to implement them might be given by signalling a codeword in clear, or by voice over a radio net or by telephone. Occasionally there may be a matter of such secrecy that knowledge of its existence must be limited to few people. In these circumstances a wide knowledge of the codeword might excite unwanted curiosity. When this is the case, the codeword itself should be given a protective marking, although not necessarily as high as its meaning. When a codeword marking is applied, the asset or event must attract a protective marking of RESTRICTED as a minimum.

9. **Security of Codewords in Use.** Users must ensure that:

a. Protective markings of codewords and their meanings are progressively downgraded as the need for secrecy of plans, projects or operations diminishes.

b. A codeword together with its meaning must never feature in any electronic transmission such as a signal, telegram, telex, fax or telephone conversation, although they may appear in the same document, provided the document is correctly protectively marked.

c. Codewords in frequent use on a wide distribution are changed from time to time as a protection against possible compromise.

10. **Exercises.** If, for real security reasons, codewords as opposed to nicknames, are required for exercises, they should be issued by commands from the list of those allotted by the DCMC. Care should be taken in defining the meanings of codewords used on exercises particularly if there is a likelihood that it may become necessary later to release codewords and their meanings to the Press. A codeword used for an exercise must always be prefixed by the word EXERCISE, for example, EXERCISE MATADOR. Nicknames only are required for RESTRICTED exercises.

11. **Cancellation of codewords.** Users are responsible for notifying the issuing authority, through normal channels, of the cancellation and surrender of a codeword when its purpose has been completed or it has been replaced after compromise. This notification should include the protective marking retained by the meaning. Surrendered codewords must in no circumstances be taken into use again without specific re-issue by the issuing authority.

12. **Compromise of codewords.** If a codeword is compromised, the appropriate Principal Secuurity Adviser must be informed immediately. To minimize any risk of compromising, a new codeword should not be referred to in the same document as the one it is replacing. When a change of codeword becomes necessary all concerned must be informed that the original has been cancelled and will be replaced by a new codeword to be contained in a later communication. A used codeword will not be reallocated for at least 3 years (or, if the branch concerned so requests, for a period up to a maximum of 5 years) after cancellation. It will be reallocated only if there is no suitable codeword available and if the controller is satisfied that its further use will not cause misunderstanding. The second communication should be given the same protective marking as the meaning of the codeword and should merely refer to the first communication and state `Codeword is ...'

13. **Use of codewords for equipment after declassification of the meaning.** A codeword allotted to an equipment may be continued in use, if appropriate, as a name for the equipment after it has been declassified.

14. **Handling of codewords.** Codewords are to be handled as CONFIDENTIAL until they are taken into use and allotted a new protective marking by the user.

15. **Use of nicknames.** The use of nicknames is limited to RESTRICTED and unclassified matters, examples of which are:

a. **Operations.** Enemy locations and target indication.

b. **Training.** Names for exercises.

c. **Administration.** Titles for logistic projects, routes for movement, geographical locations and place names.

16. **Selection, notification and cancellation of nicknames**. The user of a nickname is responsible for its selection, notification, use and cancellation as follows:

a. It must consist of two words chosen at random which must be distinct and which cannot be run together into a single word (eg. GREAT COAT or PIG SKIN are not to be used). This is to avoid confusion with codewords.

b. Notification is to be limited to those concerned with the matter to which the nickname refers.

c. Nicknames do not need to be reported to the Ministry of Defence or Command headquarters.

Protection of compartmented information

17. For some categories of sensitive material or externally sourced material, generically referred to as compartmented information, but often referred to as Codeword material, in addition to the general requirements for IT system and site accreditation from the designated Accreditor(s), approval is also required from all relevant Control or Release Authorities before the material may be stored, processed or forwarded on IT system(s).

18. Compartment approval. This may be referred to by 3rd parties (i.e. those outside MOD) as an "accreditation", but within MOD the term accreditation is reserved for the activity of ensuring that the IT systems are implemented to meet the needs of UK protectively marked material at the High Water Mark of any and all compartments to be used, which is carried out by the Defence Security Standards Organisation (DSSO).

19. Risk assessment. The only compartmented information which has a MOD recognised Risk Assessment methodology is the STRAP system as laid down in JSP440 Volume 5. In order to assess the overall security requirements for other Compartmented data, a STRAP Equivalent Level (SEL) should be derived before discussing protection requirement with security staffs. Advice on the selection of an appropriate SEL can be obtained from Head of InfoSy(Tech), MB4154, 84505MB.

20. Compartmented INFOSEC representative. Where the compartmented information has a formal Control or Release Authority, a Designated Security Authority (DSA) or Cognizant Security Authority (CSA) will normally fulfil the capacity of a Compartment Infosec Representative (CIR) for the material concerned, acting as a competent authority on behalf of the Control / Release Authority.

21. In the cases of compartmented information where the UK Control or Release Authority resides within MOD, for instance the ATOMIC system, the DSA must be drawn from the staff of the DSSO. The Control / Release Authority is responsible for nominating their CIR(s), and the details of this nomination must be supplied to the DSSO in accordance with the format laid down at Appendix 1 to this Annex. In selecting an agent, the following metric should be used:

a. Where the system(s) processing the compartmented information are solely contained within the real estate of a single Principal Security Adviser, that authority should be asked to acts as the CIR;

b. Where the system(s) processing the compartmented information cross Authority boundaries, either within or without MOD, including NATO or Other Government Departments (OGD), D Def Sy should be consulted, and may in some cases elect to nominate a DD Def Sy(Info) staff officer to fill this capacity.

22. Compartmented information not solely controlled within MOD, for instance STRAP, will have their own arrangements for appointment of CIRs, and any queries should be addressed to Head of InfoSy(Tech), MB4154, 84505MB.

23. Where a requirement to process information from a compartment is identified, but the CIR is not known to the project office, then Head of InfoSy(Tech) should be consulted.

24. Incident handling. If any security incident occurs affecting systems used to store, process or forward compartmented material, then in addition to any local reporting arrangements, the MOD Joint Security Co-ordination Centre (JSyCC), which has overall responsibility for such matters on behalf of the Departmental Security Officer, must also be informed immediately. JSyCC can be contacted on 020-7218-0117 (80117MB).

This page is intentionally left blank

ANNEX L TO
CHAPTER 4

INTERNATIONAL DEFENCE ORGANISATIONS AND INTERNATIONAL ORGANISATIONS

INTERNATIONAL DEFENCE ORGANISATION MARKINGS

General

1. International defence organization (IDO) documents are those which belong to the defence organizations of the North Atlantic Treaty Organization (NATO) including the North Atlantic Cooperation Council (NACC)/Partnership for Peace (PfP) or the Western European Union (WEU). The United Kingdom is a member of both organizations. Documents are marked NATO, NACC, PfP or WEU as appropriate and are circulated on a need to know basis within the IDOs concerned. These documents are subject to certain security procedures and to the regulations of these organizations.

2. The IDO markings NATO, NACC, PfP or WEU immediately precede the protective marking as follows:

a. **NATO documents.**

(1) NATO UNCLASSIFIED

(2) NATO RESTRICTED

(3) NATO CONFIDENTIAL

(4) NATO SECRET

b. **NACC documents.**

(1) NACC UNCLASSIFIED

(2) NACC RESTRICTED

(3) NACC CONFIDENTIAL

(4) NACC SECRET

c. **PfP documents.**

(1) PfP UNCLASSIFIED

(2) PfP RESTRICTED

(3) PfP CONFIDENTIAL

(4) PfP SECRET

d. **WEU documents.**

(1) WEU UNCLASSIFIED

(2) WEU RESTRICTED

(3) WEU CONFIDENTIAL

(4) WEU SECRET

3. NATO and WEU documents which are protectively marked TOP SECRET are also marked with the IDO markings COSMIC or FOCAL respectively, as follows:

a. **NATO documents.**

COSMIC TOP SECRET

b. **WEU documents.**

FOCAL TOP SECRET

4. The meanings of the protective markings (or classifications) are similar to those given at para 0103 of Chapter 1 with the exception that the degree of compromise relates to the international organization concerned and not to the Nation. Should NATO or a partner country wish to restrict distribution on certain NACC/PfP information, this will be indicated by NATO/name of country ONLY on a separate line immediately below the protective marking, eg.

PfP CONFIDENTIAL

NATO/POLAND ONLY

5. NATO documents containing certain information dealing with nuclear matters are given the restrictive marking ATOMAL.

6. **Control officers.** A sub control officer, who is appropriately cleared, is to be appointed in each establishment which is required to handle accountable IDO documents.

Handling procedures

7. **Accountable IDO documents.** Accountable IDO documents require special handling and safeguarding in accordance with instructions issued on a `need to know' basis. Accountable IDO documents must not be filed with National protectively marked documents since the holder may be required to produce them to an IDO inspecting officer who may not be a United Kingdom National. Accountable IDO documents are:

a. NATO documents marked COSMIC TOP SECRET.

b. NATO documents marked ATOMAL.

c. WEU documents marked FOCAL TOP SECRET.

8. When there is no longer need to hold an accountable IDO document, in the United Kingdom it is to be returned to the appropriate IDO sub-registry and forwarded to the Ministry of Defence (DIS Sy IDR) for destruction. Elsewhere, local security instructions should be consulted.

9. IDO accountable documents are to be stored at the standards required for United Kingdom TOP SECRET material.

10. **Non-accountable IDO documents.** Non-accountable IDO documents need not be registered or kept separately from National documents unless they are permanently attached to accountable IDO documents. Files containing non-accountable IDO documents or extracts must however be clearly marked on the outside as follows: `This file contains NATO (or WEU, NACC or PfP) information' as appropriate.

11. Separate MOD Forms 102 are to be used for registering IDO accountable documents.

Classification and markings

12. **Correct use of markings.** It is important to use IDO markings correctly because documents so marked are authorized for circulation on a `need-to-know' basis within the IDO concerned and have to be accounted for to it; they are liable to inspection by an international team from the IDO concerned. Incorrect marking may give an IDO the responsibility for documents that are of concern to the United Kingdom only, and, in the event of the loss of such documents, for the subsequent reports and investigations which correctly should be the responsibility of the United Kingdom.

13. The markings NATO, NACC, PfP,COSMIC, WEU, FOCAL or ATOMAL are only to be placed on United Kingdom originated documents when:

a. The document is specifically prepared for issue direct to an IDO. In such cases only the copies for the IDO are to be given the appropriate IDO marking; copies retained for National use are **not** to be so marked, or

b. Copies of a document prepared for United Kingdom use are released to an IDO; only the copies sent to the IDO are to be given the appropriate IDO marking.

14. **Reversion to lower classification when detached.** Individual parts of protected documents (and covering letters) may revert to a lower classification when detached. This is to be indicated on the parts (or covering letters) concerned, eg, `NATO RESTRICTED when detached'.

15. **Covering letters.** A letter covering an IDO document is to be protectively marked at least as high as the most highly classified attachment but see para 14.

16. **Extracts.** When an extract is made from an IDO document it should be protectively marked according to the content of the extract using the appropriate IDO protective marking, eg, NATO SECRET. If the information extracted was originally supplied by the United Kingdom a National protective marking is appropriate.

17. **Downgrading.** IDO documents may not be downgraded without the consent of the originator.

18. **Copy numbering.** All IDO TOP SECRET and SECRET documents are to be copy-numbered with the total distribution shown, eg `Copy No 1 of 20'.

19. **Page numbering.** All IDO documents except those on a single sheet are to be page-numbered. IDO TOP SECRET and SECRET documents are to show the total number of pages of the whole document on the front page, eg `Total pages 14'. IDO TOP SECRET and SECRET documents are also to show the total number of pages in the main part, eg `1 of 9'; annexes and appendices are also to show this information, eg `A1 of 3' or `B2-1 of 7'.

20. **Reference numbering.** All IDO documents protectively marked SECRET or above are to bear a reference number on each page. A new annex or appendix added to a COSMIC or FOCAL TOP SECRET document, or NATO or WEU SECRET document, is to state on the first page:

a. The reference number of the original document with its date of issue.

b. The purpose of the new text, eg addition or substitution.

Transmission of IDO documents

21. Procedures governing the transmission of documents bearing such markings as ATOMAL, COSMIC and FOCAL are issued to those with a need to know.

22. IDO documents protectively marked SECRET and CONFIDENTIAL are to be handled in accordance with the rules for UK documents protectively marked SECRET and CONFIDENTIAL as set out in Annex C.

23. IDO documents marked RESTRICTED and bearing only the supplementary markings NATO or WEU are to be handled in accordance with the general rules for UK documents protectively marked RESTRICTED set out in Annex C.

Storage

24. IDO classified documents are to be stored in accordance with the minimum standards for UK documents of the equivalent protective marking (but see para 9 above).

Carriage of IDO documents by casual couriers

25. COSMIC, ATOMAL or FOCAL TOP SECRET documents are not to be carried by casual couriers (either diplomatic or non-diplomatic) in any circumstances.

Release of IDO classified information

26. NATO classified information may not be disseminated to Nations or military commands outside the NATO Alliance without the approval of the North Atlantic Council, the Military Committee or, when appropriate, the National security authority (ie the Official Committee on Security.)

27. All information exchanged under the NACC/PfP programmes is privileged information and for official use only. It will, therefore, only be disseminated to organisations and persons involved in the programmes and with a need-to-know of the information.

28. WEU classified information may not be passed outside the organization except by the originator or with his consent.

Surveys and inspections of IDO sub-registries

29. Principal Security Advisers are to ensure that surveys and inspections include IDO sub-registries and control points and associated communication centres where these are established. Inspections are to be carried out annually and will be additional to any which may be carried out by the security representatives of the IDO concerned.

30. Guidance on the method of carrying out NATO sub-registry and control point surveys and inspection is contained in NATO Document AC/35/D/1006 (Revised) dated 5 July 1976.

31. Separate reports on inspections of NATO sub-registries and control points are to be sent to the Ministry of Defence DIS Sy IDR for onward transmission to NATO.

Detailed rules for IDO document security

32. The full rules for handling IDO documents are set out in the following documents which are issued to, or are available for staff who need to use them:

a. **NATO:**

(1) Security within The North Atlantic Treaty Organisation (C-M(55)15 (Final)). (Note: Policy in respect of the exchange of information between NATO and NACC/PfP countries will be incorporated in this document.)

(2) Agreement for co-operation regarding ATOMIC information (C-M(64)39).

(3) Administrative arrangements to implement the agreement between the parties to the North Atlantic Treaty for Co-operation regarding ATOMAL information (C-M(68)41(5th Revise)).

(4) Special procedures for the handling of US-Single Integrated Operational Plan (SIOP) information (C-M(71)(27) (Revised) and AC35/WP75 (attached to C-M(71)(27).

(5) Handling of a ATOMAL information with classified communication centres (ACP 122 NATO Supplement No 2).

b. **WEU:**

(1) Western European Union security regulations RS 100 April 1995.

International organisations

33. **United Nations (UN).** The UN sometimes require its material to be protected and routinely employ markings (classifications) with the prefix "UN" which are indistinguishable from our own. Although the terms may be the same, the protection required may be different. Unless otherwise instructed, all UN marked material should be accorded the same level of protection as comparable UK markings would dictate.

34. Any messages handed in to a UK commcen for transmission over UK channels are to be protectively marked in accordance with current UK regulations. Any messages handed in with the prefix "UN" for transmission over such UK channels are to be returned to the originator with a request that the prefix be deleted and the appropriate level of protection according to current UK regulations be inserted. Messages prefixed "UN" may of course be passed over UN provided and protected channels.

ANNEX M TO CHAPTER 4

SECURITY INSTRUCTIONS FOR HOMEWORKERS

Introduction

1. These instructions are designed to ensure that the minimum standards which protect information in MOD offices are applied, as far as possible, in home circumstances and a copy will accompany all letters of appointment for homeworkers. They may not be relaxed and may be applied only in Great Britain. These rules will also apply to those MOD office-based employees who **regularly** take work home.

General

2. Homeworkers are permitted to have access to official information with a protective marking up to and including RESTRICTED, provided:

a. He or she understands his/her obligations in respect of physical and procedural security measures necessary to protect such material; and

b. All the necessary practical arrangements, as called for by the security staff, have been made to ensure they can be fulfilled.

3. Before homeworking commences the homeworker must provide his or her line manager with a written agreement to a visit to the home (and, thereafter, to periodic spot checks) by representatives of the Principal Security Adviser's staff to confirm that satisfactory physical and procedural security measures are in place. Such agreement must be confirmed whenever regular access to official information is involved, irrespective of its protective marking level.

Personal security

4. Homeworkers should be especially careful not to draw attention to the fact that they are working on official information at home. As homeworkers will have few opportunities to discuss work problems with colleagues, they may be more vulnerable to compromise by someone professing to show an interest in their work. They need to be alert to this danger, and any instances of outsiders (or those without a "need to know") showing undue interest should be reported to the appropriate Principal Security Adviser's staff.

Security in the work area (Including Storage of Information)

5. Many aspects of security which are taken for granted in MOD buildings and establishments are difficult to replicate in the home. As far as possible, homeworkers must adhere to the following guidelines:

a. Where possible, a lockable room should be set aside as a working area, used exclusively for official work. If this is not possible, a working area should be selected to minimize, and control, unexpected interruptions from family or visitors.

b. If interruptions occur during official work, the homeworker should ensure that official documents, and particularly protectively marked documents, are covered so that they cannot be overlooked.

c. When not working on official documents, they should be stored in an appropriate locked container exclusively for the protection of MOD documents (the key(s) to which must be held personally by the homeworker and spare keys to be deposited with the line manager/ESyO of the parent establishment), unless:

(1) The homeworker intends to return to it after a short interval; and

(2) It is in a room to which the door and windows have been locked; and

(3) The homeworker remains in the home.

Telephone Security

6. Homeworkers should be alert to the dangers of passing protectively marked information of possible use to terrorists, for targeting purposes, over the public telephone network. Always confirm the identity of originators/recipients of telephone calls. To minimize risk of eavesdropping, party-lines or multi-extensions are not advisable. Similarly, use of radio telephones (including cordless and cellular telephones) for passing RESTRICTED information is prohibited. The following table addresses the precautions necessary when using the telephone to discuss protectively marked information:

Type of Telephone Call			
	Within Mainland UK Excluding Northern Ireland	To & Within Northern Ireland	Overseas
Protective Marking	RESTRICTED	UNCLASSIFIED	UNCLASSIFIED

Facsimile Transmission Security

7. The considerations outlined in the previous paragraph also apply to facsimile transmissions. Where the need for speed is paramount, an officially approved facsimile machine located in the home may be used for passing information protectively marked up to and including RESTRICTED over networks within the UK. The homeworker must verify that the recipient is ready to receive the message prior to transmission. Unprotected circuits outside the UK and Northern Ireland are only to be used to transmit UNCLASSIFIED information.

Computer and Word Processor Security

8. The use of a personal computer or word processor for RESTRICTED or other official information should be approved by the parent establishment IT Security Officer (ITSO). If approved for use at home, the ITSO will issue a site specific Security Operating Procedures (SyOPs). Staff should consult JSP 440 Volume 3 for detailed instructions on the use of such equipment.

Photocopying/printing

9. It is important to keep copies of documents to the minimum necessary for the proper conduct of business. Reproduction of RESTRICTED and above documents may only be undertaken on an approved photocopier. UNCLASSIFIED documents may be reproduced on local commercial copiers if operated by the homeworker, care being taken to ensure, as far as possible, that documents are not read or identified as MOD/official documents by others.

Posting Documents - to, from and between Homeworkers

10. The minimum standards for transmitting documents, within Great Britain, through the postal services are as follows:

Protective Marking	Enveloping, sealing and marking	Approved means
RESTRICTED	Single envelope. Full address (including post code). Security markings are not to be shown.	Ordinary letter post.
RESTRICTED (plus Descriptor(s)	As above. Address by name and mark "Personal For:"	As above.
UNCLASSIFIED	As for RESTRICTED.	As above.

11. The homeworker's attention is also drawn to Annex C of Chapter 4 for full details on postal arrangements to locations in Northern Ireland and overseas and the use of return addresses on official mail.

Carriage - by the Homeworker and other MOD Staff

12. Where it is necessary to remove RESTRICTED documents from the home (to attend a meeting, for example), it should be carried in a locked container such as a briefcase with a combination lock. The container is to bear a label securely attached to the outside giving instructions to the finder. Only one side should normally be visible, the reverse being obscured by a protective cover. The visible side of the label is to read:

"IF FOUND, PLEASE SEE INSTRUCTIONS ON THE REVERSE SIDE OF THIS LABEL". The reverse side is to read: "ANYONE FINDING THIS CONTAINER IS ASKED TO TELEPHONE 0171-21-86806 OR HAND IT IN AT THE NEAREST POLICE STATION OR RAILWAY STATION OR OTHER TRANSPORT AUTHORITY WITH A REQUEST THAT THEY SHOULD TAKE THAT ACTION".

Note: The telephone number given is that of the security control room, MOD Main Building. The number of the appropriate Principal Security Adviser may be given instead.

13. While carrying protectively marked documents, the container should remain in the homeworker's possession at all times. Protectively marked documents are not to be read in any public place or on public transport.

Note: Never journey abroad or to Northern Ireland carrying a briefcase bearing the Royal cipher.

Review of Holdings

14. The homeworker should minimize official documents held at home. Holdings should be reviewed at least every six months and, where appropriate, forwarded/returned to the MOD.

Destruction of Waste

15. UNCLASSIFIED paper waste may be disposed of by shredding or tearing it into small pieces and placing into household waste bins; it must be well mixed with domestic rubbish. It must not be used as "rough" paper for use by other members of the homeworker's household. RESTRICTED paper waste must be disposed of by a method approved of by the appropriate Principal Security Adviser's staff or returned to the MOD for secure disposal. All non-paper waste must be returned to the MOD for secure disposal.

Files and File Lists

16. MOD practice should be followed. Lists of all files held at home should be kept by both the homeworker and his/her line manager's Registry to facilitate spot checks.

This page intentionally left blank.

ANNEX N TO CHAPTER 4

CASUAL COURIERS - PROHIBITED ITEMS

1. Casual couriers who have been granted a single journey - casual courier passport (with diplomatic immunity) for the purposes of carrying protectively marked material overseas are to be aware that the following items are prohibited from being carried in their diplomatic bag:

a. Contraband, including controlled substances (particularly narcotics and dangerous drugs).

b. Firearms, explosives, ammunition or other material hazardous to personnel.

c. Combustibles.

d. Liquids, foodstuffs and perishable items.

e. Currency, military payment certificates, bonds, securities, gold, silver, jewels, jewellery, postage stamps in quantity or other negotiable instruments.

f. Office equipment and office supplies, including blank forms and paper.

g. Supply items such as blankets, repair parts, tools and clothing.

h. Tobacco and alcohol.

2. Casual couriers travelling within the United Kingdom, and those who have not been granted diplomatic immunity but have nevertheless been authorised by their relevant Principal Security Adviser to carry protectively marked documents overseas, are prohibited from carrying the following items:

a. Contraband, including controlled substances (particularly narcotics and dangerous drugs).

b. Firearms, explosives, ammunition or other material hazardous to personnel.

c. Combustibles.

d. Currency, military payment certificates, bonds, securities, gold, silver, jewels, jewellery, postage stamps in quantity or other negotiable instruments.

This page intentionally left blank

CHAPTER 5

PHYSICAL SECURITY

PHYSICAL SECURITY

This page intentionally left blank.

CHAPTER 5

GENERAL PHYSICAL SECURITY

INTRODUCTION

Layout of Chapter 5

05001. This chapter is set out in 18 sections following a similar format to the Cabinet Office base-document, the Manual of Protective Security (MPS). It is so set out to allow for simple amendment of the individual parts of the physical security chapter following changes in policy. Each section has a paragraph at the beginning entitled 'Further advice, information and guidance' the purpose of which is to help the user in the following ways:

a. Identify other documents that contain policy direction or more detail on the subject if so required.

b. Notify the user that certain documents must be used in conjunction with the Defence Manual of Security (DMS).

c. Identify other chapters, sections and parts of the DMS which contain additional information for the user.

d. Notify the requirement, where applicable, for the involvement of TLB security staff by an establishment in the decision making process at the earliest opportunity (e.g. in the procurement process for automatic access control systems (AACS), closed circuit television (CCTV), intruder detection systems (IDS) etc).

Definition of Physical Security

05002. In general terms, physical security means the positioning of obstacles to prevent:

a. Unauthorised access to official material.

b. Unauthorised access to property for the purpose of destroying, disabling, compromising or removing it, with the object of impeding operations, or in the pursuance of espionage or personal/financial profit.

c. Unauthorised access to official information of Defence property for the purpose of killing or injuring Defence personnel or damaging or destroying Defence property.

Nature and Scope

05003. There is no standard method of providing physical security within the MOD. To give all establishments equal protection would be wasteful. The degree of protection will vary from area to area and HOE must determine their own requirements based on advice from the appropriate security organisation within the minimum baseline measures described fully in section I of this chapter and such other regulations that are promulgated from time to time. The physical security of Defence establishments is to be provided by a balanced mix of physical security measures such as:

a. Fences.

b. Lighting.

c. Perimeter intruder detection systems (PIDS).

d. Intruder detection systems IDS).

e. Automated access control systems (AACS).

f. Guards.

g. Guard dogs.

h. Locks and containers.

i. Control of entry.

j. Secure rooms.

k. Hardened buildings.

l. CCTV.

Physical security measures are not primarily intended to prevent or deter attack by overt military action.

Monitoring

05004. A system of regular surveys, inspections, reviews and checks is to be implemented to ensure that physical security measures are well organised and maintained as a part of the overall protective security of an establishment.

Defence in Depth

05005. The physical security measures chosen as a result of the risk analysis (RA) (see Chapter 3) and minimum baseline measures methodologies carried out by an

establishment should be arranged so as to be mutually supporting. Additional measures may be required to achieve the degree of protection necessitated by:

a. The designation of an establishment as a Key Point (KP).

b. The security categorisation of an establishment (see Chapter 2).

Basic Principles

05006. The following basic principles apply:

a. Physical security measures are more effective and less costly if they are incorporated in the design stage of new projects. It is appropriate, therefore, to plan for higher levels of threat.

b. Where cost effective, maximum use is to be made of security equipment such as IDS, PIDS and AACS.

c. Protectively marked information and equipment is to be concentrated in as few places as possible.

d. Physical security systems are to be related to operational needs and administrative requirements.

e. Security measures must produce defence in depth.

Responsibility for Physical Security

05007. Responsibility for physical security within Defence establishments is as follows:

a. **Directorate of Defence Security.** D Def Sy is responsible for the issue of security policy for physical security for the Defence estate.

b. **Top Level Budget Holder.** The TLB Holders are responsible for the implementation of security policy at establishments within the Defence estate. Each TLB Holder will have a Principal Security Advisor (PSyA) within his staff.

c. **Head of Establishment (HOE).** Responsibility for physical security measures rests with the HOE who is advised as appropriate by the establishment security officer (ESyO), specialist security unit and/or TLB PSyA.

d. **OIC buildings, unit commanders, branch and establishment/unit security officers.** These office holders are responsible for ensuring that the requirements of this chapter are applied within their areas of responsibility.

They are to ensure that physical security is properly enforced at all times and that orders exist for duty checkers/guards.

e. **Individual responsibility.** It is the personal responsibility of all Service and MOD civilian personnel, attached members of other Services and Crown employees serving with them, to ensure that all prescribed physical security measures are correctly applied and to take the appropriate countermeasures when breaches of security occur or are suspected.

Security Orders and Plans

05008. HOE are responsible for ensuring that their establishment has comprehensive security orders and plans readily available to and which are signed as having been read and understood by appropriate personnel.

The Minimum Baseline Measures Matrix

05009. As a result of the Review of Protective Security (RPS), physical security measures, which will indicate the adequacy of the security measures on the establishment according to a given threat level, are given points according to the minimum baseline measures matrix. Full details of the matrix and how it is to be used are contained at Section 1. In particular the following is to be noted:

a. The matrix is primarily designed to counter the **ESPIONAGE** threat, although some of the measures applied will afford a degree of counter terrorist, sabotage and criminal damage defence. Its use is mandatory for the protection against compromise of confidentiality. The risk management process detailed in Chapter 3 will determine its use for 'integrity' and 'availability'.

b. The matrix is to be used at LOW THREAT unless establishments are notified otherwise by PSyAs following advice from D Def Sy.

c. Notwithstanding sub para b. above, the threat to certain sensitive establishments may be considered to be at higher than LOW. PSyAs may dictate to certain establishments what threat level they face.

d. Establishments are to follow the **SPIRIT** of the baseline measures matrix at all times. HOE are not to allow nonsensical situations to arise such as the fitting of a high standard of lock to a standard office door with glass panes, in order to score more points on the matrix, which would allow other normal security precautions to be dispensed with.

Anomalies with the Matrix

05010. Anomalies may arise in the application of this new methodology which may require amendment in due course. Any apparent anomalies are to be notified by establishments to TLB PSyA for onward staffing to D Def Sy.

Reference Documents

References in Manual

05011. A list of the documents referred to in this Chapter is at Annex A.

Security Units

05012. Establishment security staff should use the services of their appropriate security units when required, in the implementation of the policy in this Chapter. It is not expected that all appointed ESyOs will have the specialist security knowledge and/or security staff to be able to implement, without specialist security unit advice, the instructions contained in the Chapter. The role of the appropriate single-Service security units/TLB PSyA staffs in the implementation process is, therefore, important.

Conflict of Standards

05013. Where there is a conflict of physical security standards between JSP 440 and other security instructions, the more rigorous standard will prevail unless specifically notified otherwise.

This page intentionally left blank

SECTION I TO CHAPTER 5

GENERAL PRINCIPLES

Introduction

General

05101. This section of Chapter 5 contains instructions for the physical protection of information and equipment against attempts to acquire them illicitly by surreptitious attack or theft.

Defence in Depth

05102. Physical measures represent only one aspect of protective security and they need to be supported by sound personnel, document handling, communications and computer security. Sensible management of security risks involves finding the most effective (and cost effective) ways of countering the given threats by a combination of measures from each of these areas. Good physical protection, preferably built into any site or building from the beginning, is of fundamental importance.

Risk Management and Minimum Baseline Objectives

05103. Risk management offers a high degree of flexibility in providing the levels of protection required to safeguard protectively marked assets. To ensure that there is some degree of consistency and mutual assurance about the way one establishment's assets are handled by another, certain minimum baseline objectives apply to all areas of protective security. They are intended to provide acceptable security at all levels of protection where the threat is assessed as 'Low'. Further information on risk management can be found in Chapter 3.

The Minimum Baseline Measures Matrix (MBMM)

Meeting Baseline Objectives

05104. The matrix and menu of minimum baseline measures for physical security at Annexes A and B provide a range of options which meet the baseline objectives. They are designed to help the management of security risks by offering a means for the identification and selection of the most suitable and cost-effective physical security measures to safeguard protectively marked material against attempts to acquire them illicitly by surreptitious attack or theft. Although many of the measures suggested will be helpful in a counter-terrorist context (and suitable counter-terrorist measures already in place may be taken into account in meeting the baseline measures), the weighting given to the measures in the matrix is not **primarily** intended to meet terrorist threats. The matrix and menu are intended as a guide and particular circumstances may require different solutions. The achievement of a minimum score cannot be taken to be a substitute for a sound assessment of security measures based on the importance of the assets, the conditions and layout of the site, the level of the threat and protection required. Local circumstances may dictate that, despite an adequate score, enhanced

measures or alternative combinations of measures should be considered. (See also para 05009.)

Threat Levels

05105. The minimum baseline measures are those in the first column of the matrix (headed L). The remaining columns offer a means of deciding on the increased measures appropriate to levels of threat higher than Low. ESyOs are to keep themselves regularly up-to-date on the nature and levels of threat to their assets (by consulting their appropriate PSyA and local Service and civil police authorities); and are to decide for themselves on the proper response to increased levels of threat, in the light of local circumstances.

About the Matrix

05106. The minimum baseline measures are set as numerical values within a matrix, which correspond to the level of protectively marked material and to the level of the threat. The matrix, as shown at Annex A, is supported by a menu of physical security measures (Annex B) from which measures can be selected so that the sum total of the value of the individual measures equals or exceeds the required numerical value of the appropriate minimum baseline measures. It is a fundamental principle that points are only valid when correct security procedures and practices accompany the selected measure.

Numerical Values

05107. The numerical value of the baseline measures required for each level of the protective marking system is made up from different sections of the menu of measures: 2 from mandatory sections of the menu of measures and the remainder from any of the sections. This system of mandatory and additional measures is to ensure that a sensible balance of measures is achieved and allows HOEs flexibility in the measures they apply to reach the baseline position, taking into account the security facilities, equipment and manpower at their disposal.

How the Matrix is Used

05108. The matrix is used by selecting the appropriate level of protectively marked material and then reading off the scores to be achieved against the mandatory and additional sections of the menu of measures. Having identified the points score required, the user should then turn to the menu of measures. A minimum baseline measures matrix points check sheet for use by ESyOs is at Annex C. A guide to the use of the minimum baseline measures matrix is at Annex D and a sample of how to complete the full documentation is at Appendix 1 to Annex D.

Menu of Measures

Sections

05109. The menu of measures is divided into 6 sections, each dealing with a particular aspect of security (or layer of 'defence in depth'). For ease of application, the menu is laid out as a proforma with scores (loading) provided for various options. Spaces are also provided for inserting the various points scores.

Weighting of Measures

05110. Some measures are weighted in that their points score multiplies with that of another measure (eg containers and locks), whilst others are added (eg fences, Perimeter Intruder Detection Systems, lighting and CCTV). The value of zero is used as a multiplier where a fence has no control of entry at its entry/exit points. Where control of entry is provided, the multiplier of one will validate the points awarded to the fence.

Selection of Measures

05111. In deciding what measures to select, the user is to include existing security measures and then fill in the score obtained. The results can then be compared with the requirements of the matrix. From the comparison it will be apparent whether the measures are excessive, adequate or need supplementing.

Additional Measures

05112. If additional measures are required, establishments are to decide which measures to select in the light of the actual threats faced by them. If there is a threat from forcible attack, for instance, the strength of a container may be a higher factor than the Class of lock; conversely, if the threat is from surreptitious attack, a high class lock may be a more important factor than the strength of the container. Used in this way, with imagination and common sense, the menu will help ESyOs to find the measures most appropriate to their particular situation, the threats they face and the resources available.

Physical Security Measures - Performance Standards & the MBMM

05113. The descriptions given below (and which are used in the menu to the MBMM) are a guide to the levels of performance offered by different Classes of equipment, buildings or precautionary measures. The 4 classes of performance standard used in these descriptions are based on those being introduced into certain European standards and do not relate to those previously used to designate the performance of approved UK security equipment. Details of the type and specification of approved security equipment falling within the classifications below and which have been tested against both surreptitious and forcible attack are contained in the 'Catalogue of Security Equipment'. Copies of this document are issued to PSyAs and other security staff. A summary of the names of approved containers, locks doors and other security equipment is at Annex E.

Matrix Section 1 - Containers and Security Locks

Security Containers

05114. Containers are classified according to the level of security they offer, Class 4 being the highest and 1 the lowest. The classifications of containers can be described as follows:

a. **Class 4 containers.** These are HIGH SECURITY containers which:

(1) Have a high degree of resistance to an attacker using force and fully equipped with hand and power tools.

(2) Offers resistance to the prising of doors, drawers or lids to facilitate a fishing or probing attack.

b. **Class 3 containers.** These are MEDIUM SECURITY containers which:

(1) Offer a degree of resistance to an attacker using force and having access to a limited range of hand tools.

(2) Resist flexing, twisting or jolting that will distort the carcass and allow the insertion of probes or devices in order to gain access to the container.

c. **Class 2 containers.** These are SECURITY containers which are :

(1) Of substantial design and construction.

(2) Offer resistance to the casual or opportunist attacker who has not been prepared for the attack and only has use of items that are readily to hand.

d. **Class 1 containers.** These are general purpose containers which have no particular security design features but which are lockable and are judged to offer a level of privacy.

Security Locks

05115. Security locks are classified according to the level of protection they offer, Class 4 being the highest and Class 1 the lowest level.

a. **Class 4 locks.** These are HIGH SECURITY locks which have a high degree of resistance to expert and professional attack using exclusively developed skills and resources judged not to be available commercially.

b. **Class 3 locks.** These are MEDIUM SECURITY locks which have a high degree of resistance to expert and professional attack using skills and resources that are available commercially to a professional locksmith.

c. **Class 2 locks.** These are SECURITY locks which have a degree of resistance to a skilful attacker having minimal resources.

d. **Class 1 locks.** These are QUALITY locks having a moderate degree of resistance to unauthorised opening.

Note: All keys to security containers must be held securely in accordance with the instructions in Section XII.

Matrix Section 2 - Rooms

The Level of Protection

05116. The level of protection offered by a room will depend on the strength and structure of the walls, floor and ceiling/roof, the strength and quality of the door and its lock and the quality and protection given to any windows. The specifications and standards for strong and secure rooms are contained at Section XI; the names of the rooms by Class are shown at Annex E to this section. The types of room are described below:

a. **Strong room.** A strong room is a windowless room which:

(1) Is designed with a high degree of resistance to an attacker using force and equipped with an extensive range of hand and power tools.

(2) Will normally have walls, floor and ceiling of concrete slab construction.

(3) Has a door of steel with bolt work secured by Class 3 or 4 lock.

b. **Secure room.** A room that meets the standard for a secure room is as follows:

(1) Offers a degree of resistance to a forced attack in which a limited range of hand tools are used.

(2) Offers a high degree of resistance to a surreptitious attack.

(3) Has walls, floor and ceiling of lightweight brick or block construction or plywood and plasterboard on supporting frame.

(4) Has a door of solid wood or laminate construction fitted with a lock that offers the required level of protection (normally a Class 2 or 3 lock).

(5) Has windows fitted with laminated security glass in a suitable frame or be protected by window bars.

c. **Locked room.** A locked room is a room or office that can be locked (when left unattended) and offers a degree of protection to its contents. If the room is required to offer protection against a surreptitious attack for long periods, such as overnight or at weekends, the standard of door and its lock and the standard and locking of windows should reflect the level of threat. Normally a Class 1 lock will provide adequate protection.

Selection of Locks

05117. Locks, for use on rooms, are to be selected from the range of locks listed in paragraph 05115 above and detailed, by type, at Annex E.

Matrix Section 3 - Buildings

Building Rating

05118. Buildings are rated according to their resistance to both forced and surreptitious attack. The method of construction, material used and the security of doors and windows will contribute to the overall assessment. The Classes of building are described below:

a. **Class 4 buildings.** A Class 4 building is one of substantial construction which:

(1) Offers a high degree of resistance to a forced attack.

(2) Has walls, floor and ceiling/roof of reinforced concrete or concrete slab.

(3) Has doors of reinforced steel or wood, faced with sheet steel.

(4) Has windows kept to a minimum but where necessary are suitably protected. Their frame, fixing and glazing offers substantial resistance to a physical attack.

b. **Class 3 buildings.** A building which:

(1) Offers a degree of resistance to a forced attack.

(2) Is of solid construction, normally brick or block, on cavity wall principles.

(3) Has windows and doors of a standard equal to that of the building in its resistance to a forced attack.

Modern building techniques of pre-cast or fabricated panels or steel frame and glass, may also rate Class 3.

c. **Class 2 buildings.** A building which:

(1) Has a resistance to a forced attack.

(2) Is of lightweight construction normally single brick or lightweight block or be a substantial transportable office unit.

(3) Has doors and windows of a standard equivalent to the structure in having a resistance to a forced and/or surreptitious attack.

d. **Class 1 buildings.** A building that offers Class 1 standard of strength is normally a lightweight prefabricated structure intended simply to protect its contents and those who work in it from the elements.

Matrix Section 4 - Control of Entry to Building, Area or Site

Control of Entry

05119. Control of entry can be exercised over a site, a building or buildings on a site or to areas or room within a building. The control may be either electronic, electro mechanical, guard or receptionist control or physical barriers. More information on control of entry pass systems can be found in Section IX of this chapter and the requirements for Automated Access Control Systems (AACS) are detailed in Section X. The Classes of control of entry systems are described below:

a. **Class 4 system.** An automatic access control system (AACS) which:

(1) Offers a degree of inherent security requiring the minimum of guard oversight.

(2) Is based on the use of a card or token in association with a user unique Personal Identification Number (PIN).

(3) Is used in conjunction with an access barrier that prevents pass back and ensures "one transaction, one entry".

b. **Class 3 system.** A Class 3 entry control system is an electronic AACS which:

(1) Operates as a card and PIN.

(2) Entry is controlled by a suitable barrier that may require direct supervision by a guard.

c. **Class 2 system.** A Class 2 entry control system is one involving:

(1) Security guards, custodians, or a receptionist.

(2) Involves the use of a photograph or unique design pass entry system. Other identification documents, such as Defence Identity Cards are accepted for entry purposes.

d. **Class 1 system.** A Class 1 entry control system is one based on a locked door with access allowed by either:

(1) A mechanical or stand alone electronic push button code lock (PBCL).

(2) The issue of keys to "authorised key holders".

05120 ***Spare***

The Control of Visitors

05121. The control of visitors within a protected area where sensitive material is held or worked on or where special access control are exercised will depend on the level of security clearance of the visitor and on any special control requirements that the establishment may impose on non-staff personnel. The type of control exercised over visitors is described below:

a. **Escorted visitors.** Visitors who are required to be escorted within a protected area are accompanied at all times by an appointed escort or by personnel they are visiting. If they need to visit a number of different departments or other members of staff, they are to be formally handed over from one escort to the next with, if required, the visitor's pass being annotated accordingly.

b. **Pass/badge.** Visitors are allowed unescorted entry to a protected area, or parts of it. They are required to wear a badge/pass that identifies them as a visitor and not as a member of staff. It should be noted that a visitor badging system is only effective if all staff are also required to wear a pass.

Note: Points for 'Escorted Visitors' within the MBMM can only be scored where **all** visitors (including MOD employees) to an establishment are escorted.

Matrix Section 5 - Guards and Alarm Systems

Guards

05122. The employment of guards to protect buildings or sites provides a valuable deterrent to criminals and to those who might plan a covert attack. The guards' duties and the need and frequency of patrols will be decided by considering the level of threat and security systems or equipment that might be in place. More detailed instructions on the employment of guards and patrols are contained in Section VIII to this chapter. The types of guarding are described below:

a. **Frequent internal patrols.** A patrol that operates inside a building at random intervals, not exceeding 2 hours, is a frequent patrol. It is to follow a different route, on each patrol, so that the time and place of the guards' visit cannot be predicted. Guards are to have specific tasks to perform on the patrol such as checking locked doors and security furniture and checking external doors and windows to see that they are properly secured.

b. **Infrequent internal patrols.** Internal random patrols at intervals not exceeding 6 hours allows for 2 or 3 patrols during the night and periodic security checks during a weekend or holiday period. The first patrol is to normally take place soon after cease work and is to be concerned with checking that the site or building is properly secure. Patrol routes are to be varied so that the timing and location of the guard cannot be predicted.

c. **External patrols.** Patrols that are limited to the external areas of a site or building and which are carried out by guards who do not normally have access to the buildings are 'external patrols' only. The frequency of external patrolling will be dependent upon the particular requirements of the establishment. External patrols can be vehicle mounted or on foot and patrol the perimeter, inside or outside, and checking buildings that may be covered by an internal alarm system. The mobile patrol will also act as an immediate response force.

d. **Resident or on-site guards.** Guards that are employed to man an incident control room or guard post/guardroom, but are not required to patrol are classed as 'Resident' or 'Site' guards. They can be required to survey the protected area or parts of it either visually or by using CCTV surveillance equipment. Responding to other building alarm or monitoring systems can also be included in their duties.

e. **Visiting guards.** Guards who visit a site during the night and at weekends and carry out rudimentary perimeter checks are classed as 'visiting guards'. Such types of guard include those that may not normally be allowed to enter the site or building visited but respond by calling out the "Key Holder" in the event of a suspected intrusion.

Note: There are a further 2 types of guarding used in the security of equipment matrix; these are described at para 051818.

Intruder Detection Systems (IDS)

05123. IDS are used inside buildings in place of or to assist site guards. To be effective an IDS will have a response force that will react in the event of an alarm condition. Alarm systems have been graded according to the level of security they offer. A Class 4 system offering the highest level of security and Class 1 the lowest. More detailed information regarding IDS is contained at Section VII to this chapter. The Classes of IDS system are described below:

a. **Class 4 systems.** A Class 4 IDS is one which:

(1) Is intended for use in applications where security takes precedence over all other factors.

(2) Offers a level of protection where the intruder has to plan the intrusion in detail and have a full range of equipment capable of substitution of vital system components.

(3) Is supplemented with comprehensive physical security measures and security procedures.

b. **Class 3 systems.** A Class 3 alarm system is one which:

(1) Is used in premises where high value assets are held.

(2) Includes appropriate physical security protection.

(3) Offers protection from intruders who are conversant with intruder detection systems and have available a comprehensive range of tools and portable electronic equipment.

c. **Class 2 systems.** A Class 2 alarm system is one which:

(1) Is used in premises where the security risks of a sophisticated attack are not high.

(2) Intruders are expected to have a limited knowledge of alarm systems and have available only basic tools and portable instruments.

d. **Class 1 systems.** A Class 1 alarm system is one which:

(1) Is used in low risk premises where potential intruders have little knowledge of alarm systems and a limited range of readily available tools.

(2) Does not normally have an appointed response force and relies on a public response to a local alarm sounder or strobe lights.

Matrix Section 6 - Outer Perimeter

The Perimeter

05124. A perimeter fence forms a useful barrier and identifies the boundary of a protected or restricted area. The level of protection offered by a fence depends on its height, construction, the material used and any additional security features used to increase its performance or effectiveness such as topping, PIDS, lighting or CCTV. The type of fence used on the perimeter of a site should reflect the type of threat, ie. terrorist, criminal, saboteur, vandals. Fences are graded according to the level of protection they offer, Class 4 offering the highest security and Class 1 the lowest. Instructions for external perimeter security measures are at Section III, CCTV at Section VI and security lighting at Section III to this chapter. The types of fence attracting a particular Class are shown at Annex E. The Classes of fence are described below:

a. **Class 4 fence.** A Class 4 fence is a high security barrier which:

(1) Is designed to offer the maximum deterrent and delay to a skilled and determined intruder who is well equipped and resourced.

(2) Is designed and constructed to offer a high degree of resistance to a climbing or breaching attack.

(3) Is normally supported by other perimeter security systems.

b. **Class 3 fence.** A Class 3 fence is an intermediate security barrier which:

(1) Is designed to deter and delay a resourceful attacker who has access to a limited range of hand tools.

(2) Offers resistance to attempts at climbing and breaching.

c. **Class 2 fence.** A Class 2 fence is an anti-intruder fence which offers a degree of resistance to climbing and breaching by an opportunist intruder not having particular skills and using material and breaching items that are readily to hand.

d. **Class 1 fence.** A Class 1 fence is one which:

(1) Is designed with no particular security requirements.

(2) Is only intended to mark a boundary and to offer a minimum of deterrence or resistance to anyone other than a determined intruder.

(3) Any type of construction material or hedging is used.

Entry and Exit Searches

05125. Establishments may undertake entry searches as a condition of entry. In particularly sensitive areas, entry searching is to be designed to guard against the possibility of unauthorised electronic recording and transmitting equipment or copying equipment such as cameras or scanners being brought into the establishment. Such searches also guard against the possibility of an explosive device being carried into the establishment. Exit searches can only be undertaken in accordance with HOEs statutory powers, contracts of employment or the law relating to search (Police and Criminal Evidence Act). However such searches can act as a deterrent to the unauthorized removal of protectively marked or otherwise valuable assets from the establishment.

Gates

05126. Gates are to be constructed to the same security standard as the fence and some form of entry control must be in place otherwise the security of the fence will be negated.

Perimeter Intruder Detection Systems (PIDS)

05127. PIDS may be used on perimeters to enhance the level of security offered by the fence. PIDS may be installed as covert devices (although this is usually for aesthetic reasons) or overtly, to act as a deterrent. PIDS are inherently prone to false alarm and should therefore normally only be used with an alarm verification system such as CCTV.

Closed Circuit Television (CCTV)

05128. CCTV is a useful aid to security guards in covering large sites or perimeters. The effectiveness of such a system however will depend on the selection of suitable equipment and its installation. Detailed professional advice via PSyAs is to be sought.

Security Lighting

05129. Security lighting can offer a high degree of deterrence to a potential intruder in addition to providing the illumination necessary for effective surveillance either directly by the guards or indirectly through a CCTV system. The standard of lighting is to meet the minimum requirement and its installation be appropriate to the site conditions.

05130. More information on the protective measures of buildings is detailed in Section II, Annex G and Section IV to this chapter.

ANNEX A TO SECTION I TO CHAPTER 5

MINIMUM BASELINE MEASURES MATRIX

TOP SECRET	**L**	**M**	**S**	**H**	**VH**
Mandatory - Sections 1 and/or 2, plus 3	10	10	10	12	15
Mandatory - Sections 4 plus 5 **	6	6	7	7	7
Additional - Any Sections	2	4	4	5	6
Total	**18**	**20**	**21**	**24**	**28**
SECRET	**L**	**M**	**S**	**H**	**VH**
Mandatory - Sections 1 and/or 2, plus 3	8	8	8	10	12
Mandatory - Sections 4 plus 5 *	4	4	5	5	6
Additional - Any Sections	2	4	4	5	6
Total	**14**	**16**	**17**	**20**	**24**
CONFIDENTIAL	**L**	**M**	**S**	**H**	**VH**
Mandatory - Sections 1 and/or 2, plus 3	8	8	8	8	10
Mandatory - Sections 4 plus 5	-	-	2	3	4
Additional - Any Sections	2	3	3	4	5
Total	**10**	**11**	**13**	**15**	**19**
RESTRICTED	**L**	**M**	**S**	**H**	**VH**
Mandatory - Sections 1 and/or 2, plus 3	2	2	2	2	2
Additional- Any Sections	-	-	1	2	3
Total	**2**	**2**	**3**	**4**	**5**

Notes: ** = Each Section must score at least 2 points.

* = Each Section must score at least 1 point.

THREAT LEVELS

	VH	- Very High
	H	- High
	S	- Significant
	M	- Moderate
	L	- Low

This page intentionally left blank.

ANNEX B TO SECTION I TO CHAPTER 5

MENU OF MINIMUM BASELINE MEASURES

Measure			Loading	Remarks	
Section 1 – Container					
1.	**Container/casing:**				
	a.	Class 4	4		
	b.	Class 3	3		
	c.	Class 2	2		
	d.	Class 1	1		
Sub-score (ss1) = a, b, c or d					
2.	**Lock**				
	a.	Class 4	4		
	b.	Class 3	3		
	c.	Class 2	2		
	d.	Class 1	1		
Sub-score (ss2) = a, b, c or d					

Section score (S1) = ss1 x ss2	**NB. Multiply**	

Measure			Loading	
Section 2 – Room				
3.	**Room:**			
	a.	Strong Room	4	
	b.	Strong Room	3	
	c.	Secure Room	1	
	d.	Locked Room	0	
Sub-score (ss3) = a, b, c or d				
4.	**Lock**			
	a.	Class 4	4	
	b.	Class 4	3	
	c.	Class 3	2	
	d.	Class 2	1	
	e	Class 1	0	
Sub-score (ss4) = a, b, c, d or e				

Section score (S2) = ss3 x ss4		**NB. Multiply**

Measure			Loading	Remarks
Section 3 – Building				
5.	**Strength:**			
	a.	Class 4	5	
	b.	Class 3	3	
	c.	Class 2	2	
	d.	Class 1	1	

Section score (S3) = a, b, c or d	**NB. One figure**	

Measure			Loading	Remarks	
Section 4 – Control of entry to building, area or site					
6.	**Control of entry:**				
	a.	Class 4	4		
	b.	Class 3	3		
	c.	Class 2	2		
	d.	Class 1	1		
	e	None	0		
Sub-score (ss6) = a, b, c or d					
7.	**Visitor control:**				
	a.	Escorted	3		
	b.	Pass/badge	1		
	c.	None	0		
Sub-score (ss7) = a, b, or c					

Section score (S4) = ss6 + ss7	**NB. Add**	

Measure			Loading	Remarks
Section 5 – Guards and IDS				
8.	**Guards:**			
	a.	Point Guard	10	
	b.	Dog Patrol	8	
	c.	Frequent Internal Patrols	5	
	d.	Infrequent Internal Patrols	4	
	e.	External Patrols	3	
	f.	Resident/Site Guard	2	
	g.	Visiting Guard	1	
	h.	None	0	
Sub-score (ss8) = [(a, b, c or d)* + (e or f)*] or g* or h				
* = if applicable. Resident/site guard will only score if there has been no other score for other guards or patrols				
9.	**IDS:**			
	a.	Class 4	5	
	b.	Class 3	4	
	c.	Class 2	3	
	d	Class 1	1	
	e	None	0	
Sub-score (ss9) = a, b, or c				

Section score (S5) = ss8 + ss9	**NB. Add**	

Measure			Loading	Remarks
Section 6 – Immediate dispersal/ parking/storage area				
10.	**Fence:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	2	
	d	Class 1	1	
	e	None	0	
Sub-score (ss10) = a, b, c, d or e				
11.	**Entry control:**			
	a.	Yes	1	
	b.	No	0	
Sub-score (ss11) = a or b				

Measure			Loading	Remarks
12.	**Random entry and/or exit searches:**			
	a.	Yes	1	
	b.	No	0	
Sub-score (ss12) = a or b				
13.	**PIDS:**			
	a.	Yes	2	
	b.	No	0	
Sub-score (ss13) = a or b				
14.	**CCTV (to appropriate standards):**			
	a.	Yes	2	
	b.	No	0	
Sub-score (ss14) = a or b				
15.	**Lighting (to appropriate standards):**			
	a.	Yes	2	
	b.	No	0	
Sub-score (ss15) = a or b				

Section score (S6) = (ss10 x ss11) + ss12 + ss13 + ss14 + ss15	

Measure			Loading	Remarks
Section 7 – Outer Perimeter				
16.	**Fence:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	2	
	d	Class 1	1	
	e	None	0	
Sub-score (ss16) = a, b, c, d or e				
17.	**Entry control:**			
	a.	Yes	1	
	b.	No	0	
Sub-score (ss17) = a or b				
18.	**Random entry and/or exit searches:**			
	a.	Yes	1	
	b.	No	0	
Sub-score (ss18) = a or b				
19.	**PIDS:**			
	a.	Yes	2	
	b.	No	0	
Sub-score (ss19) = a or b				

20.	**CCTV (to appropriate standards):**			
	a.	Yes	2	
	b.	No	0	
Sub-score (ss20) = a or b				
21.	**Lighting (to appropriate standards):**			
	a.	Yes	2	
	b.	No	0	
Sub-score (ss21) = a or b				

Section score (S7) = (ss16 x ss17) + ss18 + ss19 + ss20 + ss21	

TOTAL SCORE is the sum of SECTIONS 1 to 7	

This page intentionally left blank

ANNEX C TO SECTION I TO CHAPTER 5

MINIMUM BASELINE MEASURES MATRIX - POINTS CHECKSHEET

Reference:	

Assessment		
1.	Asset assessed:	
2.	Protective marking:	
3.	Threat level:	

Points check					
4.	**Mandatory points.**				
	Section 1.	Pts required:		Pts achieved:	
	Section 3.	Pts required:		Pts achieved:	
	Sections 4 & 5.	Pts required:		Pts achieved:	
5.	**Additional points.**				
	Any Sections.	Pts required:			
	Sections 6 & 7		Pts achieved:		
6.	**Summary of points.**				
	Total Pts required:		Pts achieved		
7.	**Remarks.**				

This page intentionally left blank.

ANNEX D TO SECTION I TO CHAPTER 5

GUIDE TO THE USE OF THE MINIMUM BASELINE MEASURES MATRIX

First Actions

1. Produce a proforma that consists of the following documents :

   a. A points checksheet (see Annex C).

   b. A minimum baseline measures matrix (Annex A).

   c. A menu of minimum baseline measures (Annex B).

2. On the points checksheet fill in the following:

   a. Details of the asset to be assessed (for example 'Secret Docs in HQ Building').

   b. The current **Espionage** threat (eg 'L').

3. Using the matrix :

   a. Read off the total points required to protect the particular asset(s) at the current threat level and write the figure on the points checksheet (eg '14' for SECRET at Low; Low is the standard threat level unless otherwise directed from D Def Sy by PSyAs).

   b. Read off the mandatory points required for the sections and write the figures on the points checksheet (eg '8' for Sections 1 and/or 2 plus 3).

4. Turn to the menu of baseline measures to carry out the assessment. A sample assessment is at Appendix 1.

Carrying Out the Assessment

5. **Section 1 - container.** Using the standards of containers detailed at para 05114 and shown, by type at Annex E, determine the Class of container that the protected assets are held in and write the 'loading' figure in the sub-score column (ss1), (eg a 5'x 2' security cabinet would give a sub- score of '3'). Likewise, the lock fitted to the cabinet should be allocated a loading (insert at ss2) in accordance with the standards at para 05115 and shown, by type at Annex E. (eg a Mersey lock will give a score of '3'). The Section 1 score is achieved by **multiplying** the scores of the container and lock.

6. **Section 2 - Room.** Determine the Class of the room that the asset is held in using the standards at para 05116 and shown, by type at Annex E, and insert the 'loading' figure in the sub-score column (ss3); for example an unlocked room would attract 0 points. Similarly ascertain the 'loading' for the type of lock fitted to the room using the standards at para 05115 and shown, by type at Annex E, and insert at (ss4); for example a Chubb Mortice lock would attract 1 point. The section score is achieved by **multiplying** the scores for the room and the lock.

Notes:

(1) Establishments are to follow the spirit of the baseline measures matrix at all times. Therefore, heads of establishments are not to allow nonsensical situations to arise such as fitting a Class 4 lock to a standard office door with glass panes, in order to score more points on the matrix, which in turn would allow other normal security precautions to be dispensed with.

7. **Section 3 - Building.** Using the standards at para 05118, determine the Class of the building (its strength) and insert the loading score in the Section score column (S3). For example a modern building of pre-cast panels can attract 3 points.

8. **Section 4 - Control of Entry to Building Area or Site.** Determine the Class of the control of entry to the building, area or site using the standards at para 05119 and insert in the sub-score column (ss6). Decide the loading for the visitor control and insert in the sub-score column (ss7). The Section 4 score is achieved by **adding** the two scores together.

Example: A building where entry is allowed by the issue of keys to authorized personnel will attract 1 point. If the visitor control system is one where they are required to wear a pass identifying them from permanent staff, a further point would be gained. The total for the section would be 2 points.

9. **Section 5 - Guards and Intruder Detection Systems (IDS).** The type of patrols and guarding procedures are described at para 05122:

a. Determine the type of patrols/guarding practices in the building, area and site and insert the 'loading' scores in the sub-score column (ss8). The points scores for guards are divided into 3 areas; internal patrols, external patrols and other (resident/site guarding). Points can be achieved for an establishment that has both internal and external patrols. Any additional resident/site guard will not attract any further points where a score has been achieved for internal or external patrols.

Example: A particular building housing the protected asset may be the subject of 'Infrequent Internal Patrols' (gaining a loading score of 4) and be on an establishment that has 'External patrols' around the site (gaining a score of 3). The establishment may also have a 'Site Guard' at the incident room or guardroom; the latter would only attract points if there were no internal or external patrols. Hence the total sub-score (ss8) in this example would be 7 points.

b. Determine the sub-score for the type of IDS on the establishment, area and/or site using the standards at para 05123 and shown, by type at Annex E, and insert at (ss9).

The Section 5 score is obtained by **adding** the scores for Guards and IDS and inserting at (S5).

10. **Perimeter.** Decide what Class the establishment perimeter is using the standards at paras 05124 and shown by type at Annex E and insert the 'loading' into the sub-score (ss10); e.g. an approved 2.4m high chainlink fence with security topping would merit 2 points. If the establishment has entry control insert 1 point at (ss11); if it does not then no points are allotted. Similarly, insert the 'loading' figures for the 'yes/no' measures for searches (ss12), perimeter intruder detection systems (PIDS) at (ss13), CCTV (ss14) and lighting (ss15). The total score (S6) for perimeter measures is obtained by **multiplying** the 'loading' scores of the Fence and Entry control and then **adding** this figure to the total of the rest of the sub-scores.

Example: An Establishment has a Class 2 fence (2 points), with entry control (1 point). Entry/exit searches are carried out by guards (1 point) but the establishment does not have any PIDS (0 points). It does not have any CCTV (0 points) or security lighting to the appropriate standards (0 points). The total points for Section 6 would be as follows:

Fence	x	entry control	=	#	+	total of other sub-scores	=	#
2	x	1	=	2	+	1	=	3

Note: It is important to note that points for CCTV and lighting can only be obtained if the equipment reaches the appropriate approved standards.

Completing the Points Checksheet and Further Action

11. **Completion of the Checksheet.** After completing the baseline measures menu, complete the points checksheet by inserting the total points achieved. In addition, insert the points obtained in the 'Mandatory' sections.

12. **Action to be taken if points required baseline is exceeded.** If all of these figures exceed the 'points required' then the protected asset has adequate security and no further action is required. However, there may be scope for the ESyO, in consultation with the head of establishment, to reduce some security measures, if desired, to the baseline position and this type of review is to be actively encouraged so long as expenditure is not wasted in the pursuit of lower standards when those in force are cost-effective already. Any agreed action could be written in the 'Remarks' column of the checksheet.

13. **Action to be taken if the points required baseline is not reached.** If the points achieved figures have failed to reach the points required for either the total or mandatory section scores, then the ESyO in consultation with the HOE must

re-examine the security measures implemented on the establishment and choose higher security measures accordingly to meet the baseline position.

14. **Flexibility of the Matrix.** The advantage of the baseline measures matrix is that it allows establishments the flexibility to choose their own security measures at a given threat level as long as the baseline measure is reached and certain mandatory measures are met. It also takes into account any enhanced security measures that the establishmentt may have invested in such as AACS, CCTV or security lighting thereby perhaps allowing the costs to be reduced in other areas of security.

When to Complete a Matrix

15. **General.** The matrix is primarily intended to be used to assure the **Confidentiality** of protectively marked assets. Where similar protected assets are held in a particular type of building throughout the establishment only one menu may be required to be completed for each level of protective marking; e.g. In an establishment HQ building that houses a quantity of all 4 types of protectively marked material it may only be appropriate to complete a matrix for each type (RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET) at the current threat level. There may be no requirement to complete a matrix for each container in every building as the baseline may be able to be achieved for a particular building with a menu for each type of protectively marked material.

16. **'Standard' loading on the matrix.** Much of the 'loading' on the matrix menu of measures will be the same for an establishment for each menu completed; for example, the perimeter fence, guarding/patrols posture, entry control etc may be standard for all menus on the establishment at a given threat level.

17. **Change in threat level.** If the threat changes, the ESyO should consult the completed points checksheet and menu of measures to see if the measures in force are still adequate or, in the case of a decrease in threat, whether certain measures can be changed or dispensed with. By trying differing options within the menu for a given protected asset, the ESyO should be able to obtain any new baseline position.

Example: The threat increases from Low ('L') to Moderate ('M') and the number of points required to house TOP SECRET protectively marked material increases from 18 to 20. Assuming that a particular establishment has the minimum 18 points and meets the mandatory points (which would not change for such an increase in threat) it could meet the new baseline position by introducing 'frequent Internal Patrols' to the existing 'External Patrols' thereby gaining the 2 extra points required. Alternatively, it could choose to house all of its TOP SECRET assets in a higher Class container which when multiplied with the value of the lock would meet the new baseline.

APPENDIX 1 TO
ANNEX D TO
SECTION I
TO CHAPTER 5
MINIMUM BASELINE MEASURES MATRIX - POINTS CHECKSHEET

Reference:	STR/2031/6

Assessment		
1.	Asset assessed:	Docs in HQ Building
2.	Protective marking:	SECRET
3.	Threat level:	L

_Points check					
4.	**Mandatory points.**				
	Section 1 and/or 2 plus 3	Pts required:	8	Pts achieved:	12
	Sections 4 & 5.	Pts required:	2	Pts achieved:	16
5.	**Additional points.**				
	Any Sections.	Pts required:	2		
	Sections 6 & 7		Pts achieved:	3	
6.	**Summary of points.**				
	Total Pts required:	14	Pts achieved	24	
7.	**Remarks.**				
COULD STORE SECRET DOCS IN LOWER CLASS					
CONTAINERS WITH LOWER CLASS LOCKS AND/OR					
REVIEW PATROL ACTIVITY WITH A VIEW TO REDCUCING IT					

This page intentionally left blank.

Minimum Baseline Measures Matrix

TOP SECRET	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1 and/or 2 plus 3	1	1	1	1	1
Mandatory - Section 3	2	2	2	2	2
Mandatory - Sections 4 plus 5 **	6	6	7	7	7
Additional - Any sections	9	11	11	14	18
Total	**18**	**20**	**21**	**24**	**28**
SECRET	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 3	2	2	2	2	2
Mandatory - Sections 4 plus 5 *	4	4	5	5	6
Additional - Any sections	7	9	9	12	15
Total	**14**	**16**	**17**	**20**	**24**
CONFIDENTIAL	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 3	2	2	2	2	2
Mandatory - Sections 4 plus 5	3	3	3	3	3
Additional - Any sections	4	5	7	9	13
Total	**10**	**11**	**13**	**15**	**19**
RESTRICTED	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 3	1	1	1	1	1
Additional - Any sections	-	-	1	2	3
Total	**2**	**2**	**3**	**4**	**5**

Notes: ** Each Section must score at least 2 points.
* Each Section must score at least 1 point.

THREAT LEVELS

VH - Very High
H - High
S - Significant
M - Moderate
L - Low

This page intentionally left blank

Menu of Minimum Baseline Measures

Measure			Loading	Remarks	
Section 1 – Container/casing					
1.	**Container/casing:**				
	a.	Class 4	4		
	b.	Class 3	(3)	*Lightweight Cupboard*	
	c.	Class 2	2		
	d.	Class 1	1		
Sub-score (ss1) = a, b, c or d				*3*	
2.	**Lock**				
	a.	Class 4	4		
	b.	Class 3	(3)	*Mersey*	
	c.	Class 2	2		
	d.	Class 1	1		
Sub-score (ss2) = a, b, c or d				*3*	

Section score (S1) = ss1 x ss2	**NB. Multiply**	*9*

Measure			Loading		
Section 2 – Room					
3.	**Room:**				
	a.	Strong Room	4		
	b.	Secure Room	3		
	c.	Locked Room	1		
	d.	Unlocked Room	(0)		
Sub-score (ss3) = a, b, c or d					
4.	**Lock**				
	a.	Class 4	4		
	b.	Class 4	3		
	c.	Class 3	2		
	d.	Class 2	(1)	*Mortice*	
	e	Class 1	0		
Sub-score (ss4) = a, b, c, d or e				*1*	

Section score (S2) = ss3 x ss4	*0*	**NB. Multiply**

Measure			Loading	Remarks
Section 3 – Building				
5.	**Strength:**			
	a.	Class 4	5	
	b.	Class 3	(3)	*Pre cast panels*
	c.	Class 2	2	
	d.	Class 1	1	

Section score (S3) = a, b, c or d	**NB. One figure**	*3*

Measure			Loading	Remarks	
Section 4 – Control of entry to building, ~~area or site~~					
6.	**Control of entry:**				
	a.	Class 4	4		
	b.	Class 3	3		
	c.	Class 2	2		
	d.	Class 1	(1)		
	e	None	0		
Sub-score (ss6) = a, b, c or d				*1*	
7.	**Visitor control:**				
	a.	Escorted	3		
	b.	Pass/badge	(1)		
	c.	None	0		
Sub-score (ss7) = a, b, or c				*1*	

Section score (S4) = ss6 + ss7	**NB. Add**	*2*

Measure			Loading	Remarks
Section 5 – Guards and IDS				
8.	**Guards:**			
		Internal Patrols	10	
	a.	Frequent	8	
	b.	Infrequent	5	
		External Patrols	(4)	
	c	Frequent		
	d.	Infrequent	(3)	
		Other		
	e.	Resident/Site Guard	2	
	f.	None	0	
Sub-score (ss8) = [(a* or b*) + (c* or d*)] or e* or f				7
* = if applicable. Resident/site guard will only score if there has been no other score for other guards or patrols				
9.	**IDS:**			
	a.	Class 4	5	
	b.	Class 3	4	
	c.	Class 2	3	
	d	Class 1	1	
	e	None	(0)	
Sub-score (ss9) = a, b, or c				0

Section score (S5) = ss8 + ss9	**NB. Add**	7

Measure			Loading	Remarks
Section 6 – Perimeter				
10.	**Fence:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	(2)	Chainlink
	d	Class 1	1	
	e	None	0	
Sub-score (ss10) = a, b, c, d or e				2
11.	**Entry control:**			
	a.	Yes	(1)	
	b.	No	0	
Sub-score (ss11) = a or b				1

Measure			Loading	Remarks
12.	**Random entry and/or exit searches:**			
	a.	Yes	(1)	
	b.	No	0	
Sub-score (ss12) = a or b				*1*
13.	**PIDS:**			
	a.	Yes	2	
	b.	No	(0)	
Sub-score (ss13) = a or b				*0*
14.	**CCTV (to appropriate standards):**			
	a.	Yes	2	
	b.	No	(0)	
Sub-score (ss14) = a or b				*0*
15.	**Lighting (to appropriate standards):**			
	a.	Yes	2	
	b.	No	(0)	
Sub-score (ss15) = a or b				

Section score (S6) = (ss10 x ss11) + ss12 + ss13 + ss14 + ss15	*3*

TOTAL SCORE is the sum of SECTIONS 1 to 6	*24*

ANNEX E TO SECTION I TO CHAPTER 5

SUMMARY OF THE CLASSES OF SECURITY EQUIPMENT AND SECURITY MEASURES

Security Equipment

1. **Catalogue of Security Equipment - Change of Terminology.** As a result of the 'Review of Protective Security' the terminology used to describe the security effectiveness of certain items of security equipment listed in the 'Catalogue of Security Equipment' has changed. Items are now allocated to a Class instead of a 'Category or 'Group'. The table below will act as a conversion table until an amendment to the catalogue is issued.

2. **Reference to Security Equipment.** In using the minimum baseline measures matrix and when making reference to security equipment, users are to refer to the lists contained in the table below to determine the Class of specific items and all references in the catalogue to security 'Category' and 'Group' are to be interpreted as 'Class'. The page number column in the table refers to the corresponding page in the Catalogue of Security Equipment.

3. **Handbook of Physical Security.** The 'Catalogue of Security Equipment' is held by all PSyAs and some other security staffs and is an integral part of the 'Handbook of Physical Security'.

Containers

Page No	Description	Class
A3	Grade 1A Safe: Sizes 1,2,3 & 4	4
A12	Rosengren RCC Data Safe: RCC2, RCC3, RCC4	
	RCC5 & RCC6	4
A4	Dual Combination Lock Safe	4
A5	Heavyweight GpII Cupboard: Large and Small	4
A6	Document Chest	4
A7	Lightweight GpIII Cupboard	3
A8	GpIII Cupboard: Large 4 door & small single door	3
A9	Elite Plan File	3

A10	Vertical Filing cabinet: 2 Drawer & 4 drawer	2
A13	Large Electronic Cabinet GpIII	3
A14	Small Electronic Cabinet	3
A15	Under Desk Electronic Cabinet GpIII	3
A16	CPU Tower Cabinet GpIII	3
A17	PC Processor Cabinet GpIV	3
A18	Network CPU Cupboard GpIII	3
A19	Barton Electronic Tempest Container GpIV	3
A20	Combination Lock Keybox	3
A21	Posting Keybox	3
A11	Document Box	2
A23	Switch cover: 30 Amp & 13 Amp Switch Box	2
A24	Security Plug Box	2
A25	Circulating (Despatch) Box	1
A26	Envopak security Pouch: sizes 1,2 & 3	1

Locks

Page No	Description	Class
B3	Manifoil MkIV Combination Lock	4
B5	Medway Locking Unit	4
B6	Mersey Keylock	3
D11	Henderson Cypher Lock	3
12	Codeguard Keypad	3
B8	Ingersoll Rim Automatic Deadlock: SC10, SC12 & SC71	2
B9	Ingersoll Fire Security Lock: SC73/FS	2
B10	Ingersoll Mortice Hookbolt Deadlock: SC74 Double sided & SC76 Single Sided	2
B11	Assa Twin 6000 and Assa Twin Combi	2

B12	Tamar Locking Unit	2
B15	Avon Locking Unit	1
B16	Chubb Mortice Locking Latch: 3R35	1
B17	Chubb Hook Bolt Mortice Lock: 3M50	1
B18	Chubb Upright Two-bolt Mortice Lock: 3K70	1
B19	Chubb Horizontal Two-Bolt Mortice Lock: 3J60	1
B19A	Chubb 'Castle' Mortice Lock: 3G110	1
B20	Ingersoll Impregnable Padlock: OS 711, Cs 712, & CS 700	1
B21	Abloy Padlock: 3041	1
B22	Chubb Ava 1K42 Padlock: with Normal & Extended Shackle	1
B23	Assa Class 2 Padlock: 8mm & 10mm Shackle	1
B24	Chubb Hercules Combination: 1K57 Padlock with 7B018 Locking Bar	1
D9	Simplex Digital locks (pbcl): NL/DL 100 NL/DL 200 & NS 3000	1
D10	Unican Digital Lock (pbcl)	1
D13	Assa Codoor 2000 Lock (Electronic pbcl)	1

Rooms

Page No	Description	Class
C3	Strong Room	4
C4	Type A Secure Room	3
C5	Lightweight Type A Secure Room	3
C6	Type B Secure Room	3
C7	Lightweight Type B Secure Room	3
C8	Type C Secure Room	3

C9	Lightweight Type C Secure Room	3

IDS

Page No	Description	Class
E3	AC 12 IDS Control Panel	4
E6	CPA6 IDS Control Panel	3
E7	IDS Control Panel Aplex: 60 & 100 Zone	3
E8	IDS Control Panel Executive 1000	3
E9	IDS Control Panel Genesis 1000: 15, 60 & 100 Zone	3
-	Approved portable/transportable IDS system	2
-	Approved electric fence incorporating an IDS	2

Classes of Other Security Measures

Control of entry

See para 05119.

Fences

Description	Class
Approved weldmesh fence to a minimum height of 2.4m with approved security topping.	3
Any approved Class 2 fence to a minimum height of 2.4m coupled with an approved electric fence to an approved design combination. (See note 1)	3
Approved chainlink fence to a minimum height of 2.4m with approved security topping.	2
Approved palisade fence to a minimum height of 2.4m.	2
Approved steel profile fence to a minimum height of 2.4m with an approved security topping.	2
Approved expanded metal (XPM) fence to a minimum height of 2.4m with an approved security topping.	2
225mm brick wall to a minimum height of 2.4m or 190-220mm block wall (min density 7KN) to a minimum height of 2.4m. Both types with approved topping and of an approved design.	2

Any other fence, hedge etc. 1

Notes:

1. Depending on the design combination used, it is possible for this fence also to be considered as an IDS; thus, counting in 2 sections of the MBMM.

2. For new builds or replacements, see new CSE section.

This page intentionally left blank.

SECTION II TO CHAPTER 5

SECURITY ASPECTS OF WORKS PROJECTS AND SERVICES

General

Security Advantages

05201. Significant security advantages can be derived from the proper positioning of buildings, roads and car parks within a site. Security requirements are to be considered at the earliest stages of planning new sites or buildings, or alterations to existing buildings, since physical security measures are invariably more expensive and less effective when introduced at a later stage. It is essential that a long-term view is taken on threats when buildings are planned and commissioned.

Further Information, Advice and Guidance

05202. Where necessary, advice on the current threats and specialist counter measures may be obtained via TLB PSyAs who are to be consulted by establishments in accordance with para 05206, before detailed planning or building commences. Consideration should be given to the following:

a. **Terrorist threat and counter measures.** TLB PSyAs can obtain specialist advice on both espionage and terrorist threats via D Def Sy. Direction on the principles and requirements for the physical security of non-nuclear establishments in GB is contained in JSP 436 (direction on the security of nuclear establishments is contained in JSP 440 volume 4). Additional guidance on counter-terrorist measures is also provided in the Manual of Counter-Terrorist Measures. Specialist advice on structures, building materials, window and door design, grilles and glazing materials, use of defensive landscaping etc, required to counter them can be obtained from Defence Estates (DE) Specialist Construction Group (SCG).

b. **Criminal threat and counter measures.** Advice on local criminal threats and crime prevention may be obtained from the appropriate Service, MOD or civil police Crime Prevention Officer. Further advice is contained in the Home Office Crime Prevention Centre's guidance on Secured by Design (SBD) and the relevant Parts of BS 8220, TLB PSyA may obtain both documents from D Def Sy.

c. **Weapons and ammunition sites and buildings.** The detailed requirements for sites and buildings housing weapons and ammunition are contained in Chapter 6.

Coordination of Works Projects and Services

Background

05203. It is essential that security specifications for structures, systems and equipment needed for each project/work service are properly identified, defined and approved before contracts are let. Moreover, where systems and equipments are concerned, operational performance standards and maintenance requirements must also be included. Failure to do so may result in either inadequate or inappropriate security provision, and could lead to excessive expenditure.

Minimum Military Requirements (MMR)

05204. When determining security measures for incorporation within works services, the principle of MMR should be followed (i.e. only those measures required to meet operational, statutory or other mandatory requirements should be specified).

Responsibilities

05205. Responsibilities for providing specialist security advice for works projects and services are as follows:

a. **Directorate of Defence Security.** D Def Sy is responsible for issuing departmental policy for security aspects of works projects and services.

b. **Top level budgets (TLB) holder** TLBs are responsible for the provision of security works services and can obtain advice from their PSyAs.

c. **ESyO's responsibility to Head of Establishment.** The ESyO is responsible to the Head of Establishment or the provision of security advice within work services through the production of the SSR and OR. To assist him with this task the advice and assistance of the PSyA or other specialist security staffs can be sought.

d. **MOD DE (SCG).** DE are responsible for:

(1) Maintaining a library of all relevant security works material including drawings developed elsewhere and making it available to the relevant PSyA when required.

(2) Acting as the technical advisory service for works interfaces with security measures that could be any combination of physical, procedural and contractual measures.

(3) Works technical policy.

(4) Specialist advice on hardening buildings and services against attack. This will include glazing, robustness of buildings, location of services and bomb shelter areas.

d. Special Services Group (SSG). The role of SSG and the services that it can provide to the MOD are detailed at Annex A.

Procedures for Works

05206. Before a works project or service is undertaken, the Project Sponsor (PS), Project Staff Officer (PSO) or Property Manager (PROM) is to consult the ESyO who is to attend siting boards as required and who will, if necessary, consult the appropriate PSyA. The PSyA may wish to obtain further specialist advice. The security involvement in work services can be summarised as follows:

a. **Security involvement in works projects.** A works project is any single item of work costing more than £240,000 (excluding VAT and fees). The stages of works implementation and the associated security tasks and responsibilities for project work are set out at Annex B.

b. **Security involvement in property management.** A property management (PROPMAN) works service, is any single item of work costing less than £240,000 (excluding VAT and fees). The stages of works implementation and the associated security tasks and responsibilities for PROPMAN work are set out at Annex C.

c. **Security involvement in works related private finance initiatives (PFIs).** PFI is a procurement approach, based upon a set of principles and techniques, aimed at determining the feasibility and cost effectiveness of allowing the private sector to provide the MOD with certain capabilities and services. The stages of works implementation and the associated security tasks and responsibilities for works related PFIs are set out at Annex D (to be issued).

d. **Statement of security requirement (SSR).** The need for a SSR within the overall statement of requirement (SOR) for a project, PROPMAN or PFI work is detailed within Annexes B, C and D. Guidance on the completion of the SSR is at Annex E. The SSR will be developed in the OR and inserted into a project brief (PB) for projects or works order for PROPMAN work.

e. **Operational requirements (OR).** An OR must be completed once approval has been given by the budget holder for any security related works project or service, or for the procurement of security equipment. Within project work, the PS requires as much detail as possible in order to provide the best estimate of costs for the option study. Therefore consideration should be given to drafting an immature OR based on available information.

Guidance on the completion of the OR is at Annex E. Specific details to be addressed in ORs for CCTV, IDS and AACS are given in Sections VI, VII and X respectively.

f. Request for initial SSG advisory service. A proforma for use by TLB PSyAs to request an initial SSG advisory service in respect of security requirements at a Defence site is at Annex F. Individual establishments are not to make contact with SSG without the consent of their Security Authority.

Procurement of Security Equipments/Systems

Requirement for PSyA Approval

05207. The initial decision on the requirement for security equipments/systems will invariably be taken at establishment-level. However, for all projects involving fences (including PIDS), CCTV, IDS, security lighting or AACS, TLB PSyAs are to be consulted to ensure that the equipment is:

a. Of an acceptable standard, quality and design.

b. Capable of utilising existing technology available to the Defence estate.

c. Capable of further exploitation/upgrading in line with planned Defence utilisation of technology.

d. Good value for money **throughout** the life of the system (i.e is not just the cheapest option that subsequently proves to have expensive maintenance costs).

e. Part of a coordinated approach towards security equipments/systems for the Defence estate.

Central Monitoring

05208.

a. **Coordinated approach.** In order to avoid an 'ad-hoc' approach to the procurement of security equipments and systems throughout the Defence estate, centralised monitoring of the process must take place. The above requirements, leading to a coordinated and strategic approach can only be achieved centrally by the involvement of TLB PSyAs from the very beginning; they are part of the policy making machinery which is centred on D Def Sy for deciding the security equipment requirements of the Defence estate.

b. **Named security products.** Exceptionally, named security products may be specified by TLB PSyAs, as clauses in contracts, provided that the specific approved equipment/item is justified on security grounds.

Maintenance.

05209. To ensure any system continues to provide its optimum performance, performance testing, servicing and preventative maintenance is needed. These tasks should keep costs down and maintain acceptable performance. The frequency for each task is to be determined after consideration of the possible threat, the manufacturer's recommendations, the technical requirements of the equipment, the effort required to complete each task and the cost of carrying out the task compared to the benefits to be gained. If maintenance is not carried-out on security equipments and systems then they will fail to be regarded as one of the menu of security measures that make-up the Minimum Baseline Measures Matrix. Specific recommendations for maintenance of PIDS and IDS are contained within Sections III and VII respectively.

Pre-Acceptance Board Testing

05210. It is essential that an audit of the security system is carried out, by a security specialist qualified to do so, prior to acceptance. The requirement for a security audit should be specified in the SSR and incorporated in the PB or PROPMAN works order. Where an audit finds an unacceptable fault, it is for the PS or PROM to consider whether this is a breach of the contract for the contractor to correct.

a. **Purpose.** The purpose of the audit, which must be carried out prior to the acceptance of the facility by the Establishment, is to ensure that the security requirements specified in the PB or works order have been fully met.

b. **TLB PSyAs.** ESyOs are to consult PSyA staff about the choice of security specialist to be employed to carry out the audit of the system.

Counter Terrorist Physical Security Measures for MOD Buildings

05211. Counter terrorist physical security measures are to be applied to all MOD owned or occupied buildings; the purpose of which is to limit damage to the building fabric and injury to the occupants. It is the responsibility of TLB PSyAs to ensure that the measures applied are appropriate and take into account the location and function of the building. The minimum physical security measures are given in Annex G.

Site Selection

Factors to Consider

05212. Where a choice of locations exists for a new facility, the security advantages and disadvantages of each are to be evaluated. Factors to consider are:

a. The effect of topographical features and landscaping on perimeter security, overlooking, ease of access and communications.

b. The existence and proximity of public rights of way and neighbouring buildings.

c. The proposed use(s) of the facility.

d. Access arrangements for emergency services.

Site Layout

Security Perimeter

05213. Facilities used for work on protectively marked material are to have a defined perimeter; a physical barrier such as a security fence, wall, or hedge; or a psychological barrier designed to make any intruder feel vulnerable and exposed (for details of perimeter security measures, see Section III).

Open Space

05214. The measures that apply for open spaces within the site layout are as follows:

a. Open space between any outer security perimeter and the buildings it surrounds is to be planned so as to help patrolling, but hinder overlooking and deprive intruders of cover.

b. For similar reasons there is to be open space between buildings.

c. The foliage of tall trees should be kept well clear of the ground and of any fence. Account is also to be taken of shadows they may cast.

Car Parks and Road System

05215. The road system and car parks inside the perimeter are to be designed to reduce the need for (or eliminate the possibility of) parking vehicles near living or working accommodation. To allow continuous use during periods of enhanced terrorist threat, where possible, car parks are to be sited at least 25m from such buildings. In addition, consideration (if possible and appropriate) should be given to constructing an earth bund (as close as possible to the car park) between the car park and those buildings normally occupied. If possible, a separate visitors' car park is to

be provided away from living and working accommodation. Where underground car parks are used, access control measures must be rigidly enforced. In addition, the effects of blast in a closely confined space must be taken into account and compensatory measures taken.

Vehicle Waiting Area

05216. An area can be provided outside the main site entrance for vehicles waiting to enter. Traffic congestion can distract the guards. However, as with car parks, due consideration is to be given to the potential terrorist threat. In these circumstances, for Service establishments, waiting areas are normally to be located outside the establishment close to the point of entry. Consideration should be given to landscaping these areas to minimise the effects of the blast.

Ancillary Facilities

05217. Ancillary facilities are to be sited away from or at worst be on the periphery of areas used for protected work. Public access routes, eg for maintenance work, for the delivery of supplies or removal of refuse, are not, as far as possible, to pass through areas used for work on protected material.

Buildings with Public Access

05218. Buildings with public access should be outside the security perimeter. If such buildings have to be inside, they are to, where feasible, form part of the security perimeter. Access through them, to the rest of the site, is to be controlled.

Number of Entrances

05219. The number of entrances to a building or perimeter is to be kept to a minimum (see also Section III to this Chapter). In the case of establishments in urban areas any entrance directly off a busy street is to be avoided. There are to be separate entrances for pedestrians and vehicles. A separate goods entrance should be arranged so that vehicles can be supervised while loading and unloading.

Lighting at Entrances

05220. Adequate lighting is to be provided at entrances so that vehicles and people and their passes are clearly visible to the guards. The types of lighting are detailed in Section III to this Chapter.

Guard Accommodation

05221. Accommodation for guards is to give an unobstructed view of surrounding areas. The accommodation is to be equipped with domestic facilities; and any outdoor guard-point is to be weather proof (see Section VIII to this Chapter).

Working and Living Accommodation

05222. Working and living accommodation is to be sited well back from the perimeter and, where possible, at least 25 metres from a car park or road.

Armouries and Ammunition Stores

05223. Armouries and ammunition stores are to conform to the standards detailed in Chapter 6. The authority for ammunition stores is the Explosives Storage and Transport Committee (ESTC) or the relevant Chief Inspector of Explosives; for works aspects it is DE SCG. Likewise the works authority for armouries is DE SCG under instruction from the relevant PSyA.

Security Control Centre (SCC)

05223a. HOEs should seek to have all of their security systems fully integrated into one central command location. However, unit security plans should specify locations for emergency use if the primary location is rendered inoperable. Where considered necessary, and if manpower permits, a permanent manned SCC should be established separate from the guardroom. The SCC or guardroom should have an appropriate communications suite (e.g. radios, telephones and a PA system).

Public Address (PA) System

05223b. A PA System, which can be used by the guard force or security personnel, should be installed, where appropriate, throughout the establishment. This will allow personnel to be alerted and respond quickly and correctly to differing levels of threat or attack.

Building Finishes

05223c. Where appropriate, the inner face of perimeter walls and the lower part of building exteriors should be finished in a light coloured material to aid detection of intruders and/ or IEDs.

Accommodation Planning

Layout of Accommodation

05224. In addition to site planning, careful layout of accommodation within a building significantly enhances security. The Project Manager (PM), Establishment Works Consultant (EWC) or Works Service Manager (WSM) (in the case of PROPMAN work) should be briefed in detail by the PS or PROM, as appropriate, having been advised by the relevant PSyA. Formally and contractually all instructions to contractors must be issued by the PS or PROM, as appropriate. Throughout this process it must be remembered that due consideration needs to be made of statutory fire regulations.

Briefing of PM or WSM

05225. For each project/PROPMAN works service, the PSyA is to brief the PS/PROM on the following:

a. The location of secure rooms or secure zones.

b. The types of protection required for windows, skylights, doors and other access points.

c. Any special requirements for installations such as IDS, AACS, mechanical document transfer (MDT) or mail screening systems.

d. The security problems arising out of the installation of lifts (see para 05232), air conditioning and other ducting.

e. Where to position bulk destruction facilities if it is proposed to dispose of large quantities of protectively marked waste on site.

f. The need to minimise the risks of overlooking and overhearing (see Section V).

The PS/PROM is to brief the PM/WSM accordingly.

Protectively Marked Material

05226. The following principles are to be applied when allocating accommodation to staff working on protectively marked material:

a. **Ground floor.** The use of the ground floor is, wherever possible, to be avoided for work on SECRET or TOP SECRET material as upper floors are less vulnerable to intrusion, overhearing and overlooking.

b. **Communications and computers.** Communications centres, large computer installations, and equipment requiring TEMPEST protection is, wherever possible, to be located near, at, or below ground level. The requirements for the siting of communication and computer equipment should include the avoidance of water pipes and other sources of flooding.

c. **Registries and other areas.** Registries, workshops or other areas which may contain protected material are not to constitute passageways to or from less secure areas.

d. **Public areas.** Segregated accommodation is to be provided for members of the public eg waiting or interview rooms.

e. **Electronic and audio counter measures.** Planning is to consider the requirement to prevent electronic and audio eavesdropping from areas outside the establishment's control.

f. **Locally employed staff overseas.** At establishments overseas, arrangements are to be made to segregate locally employed staff without security clearance from areas in which protectively marked material is used.

Secure Zones

General

05227. When different degrees of security protection are required in various parts of the building, the more sensitive areas are to be concentrated into a secure zone (or zones). These are parts of a building to which entry is separately controlled. Secure zones are not to be confused with secure rooms (see Section XI of this Chapter).

Reason for Secure Zones

05228. A secure zone is established for one of the following reasons:

a. To concentrate work on protected material in one area of a building that does not itself have access control.

b. To give additional protection to an area where particularly sensitive work takes place in a building which already has a secure perimeter and to which entry is controlled.

Building alterations are only required in order to provide access control to a secure zone. Strengthened walls and doors may not be required, but security furniture or a secure room of an approved standard may be required for the custody of higher levels of protected material within the secure zone.

Inner Compartments

05229. Where an entire building or group of buildings is made into a secure zone, a series of inner 'compartments' may be created with entry to each controlled separately in one of the following ways:

a. By guards.

b. By the authorised occupants themselves.

c. By the use of an access control system.

Adjoining Rooms

05230. Several adjoining rooms can be made into a secure zone if the rooms are inter-communicating. A secure zone is to have one entrance/exit only, although additional emergency exits may be required on safety grounds. All other doors giving access to the secure zone are to be permanently secured.

Whole Floors as Secure Zones

05231. Where whole floors of a building are made into secure zones the following measures apply:

a. The secure zone is to be established on the uppermost floor or floors.

b. Roofs of such areas are to be made secure.

Lifts

05232. When access to a secure zone, comprising several floors, is by lift, the following applies:

a. The lifts are to be programmed not to proceed beyond the lowest floor of the secure zone, where a control point is to be established.

b. Lift entrance doors on the higher floors are to be kept locked.

Secure Zones Housing Protected Material

05233. Where secure zones are established to house registries of protected material the measures below apply:

a. Entry is to be confined to those who work in the registry.

b. A reception counter is to be provided near the entrance for the delivery and collection of material.

c. A separate room within the registry is to be provided where authorised staff can see and work on specially sensitive material.

Security in Open Plan Offices

Introduction

05234. The use of open plan offices creates particular problems in respect of the security of protectively marked material and the preservation of the "need to know" principle.

General Principles

05235. The threat of espionage will always exist and the risk of information becoming known to unauthorised personnel will increase in open plan offices. The following general principles apply:

a. Staff authorised to handle protectively marked material are to ensure that the "need to know" is rigorously enforced.

b. No-one may be permitted access to protectively marked information unless specifically authorised to receive it.

c. Individuals are responsible for the material with which they are entrusted at all times, and are to be aware of the risk of overhearing and overlooking, taking precautions as necessary.

d. It is permitted to work routinely on documents/material protectively marked up to SECRET.

e. Documents marked TOP SECRET and those bearing special markings are to be handled and worked upon in accordance with specific instructions.

f. Visitors are to be escorted at all times.

g. Meetings in which protectively marked information is to be discussed should not normally be held in open plan offices but be held in secure conference facilities where practicable.

Sensitive Special Projects

05236. Groups dealing with special projects of a sensitive nature are to be segregated from those groups which do not need to know; however, segregation should only take place where the amount and sensitivity of material justifies separate working areas. These separate secure areas are to be subject to access control measures. Where practicable, such areas are to be in the less accessible parts of a floor or building i.e. located away from general access doors or transit corridors. The type of access control is to depend on a group size and any specific local requirements.

Desk and Seating Arrangements

05237. Desk and seating arrangements are to be such as to ensure that access to protectively marked material by others without "a need to know" is difficult. This applies to both hard copy information and that displayed on computer screens. The arrangements are to take into account both overhearing and overlooking, internally and externally.

Unattended Workspace Overseen

05238. Where clear working groups can be identified, an individual can leave his working space for short periods (less than 30 minutes) providing his desk area is within view of an individual with the same access who can satisfactorily watch the desk. This arrangement does not relieve responsibility for the material entrusted to an individual who must ensure the material is adequately protected at all times.

Unattended Workspace not Overseen or Vacated for more than 30 Minutes

05239. In instances where a desk area is vacated for less than 30 minutes but a second individual is not available to oversee or in the event the desk is vacated for more than 30 minutes then the following measures apply:

a. Protectively marked material (including removable hard disk drives), CONFIDENTIAL or above are to be removed from sight and secured in security approved containers.

b. RESTRICTED material with or without descriptor markings is to be held under lock and key.

c. Security keys are not to be taken off site.

d. VDUs are to be switched off and any protectively marked removable media secured.

Special Handling Material

05240. There will be occasions when some individuals will hold small quantities of protectively marked material subject to special handling arrangements and to which access is limited. Such material is to be secured in document boxes with Manifoil Mk IV combination locks to prevent others having access. When not in use these boxes should always be held in another approved security container.

Sensitive Conversations

05241.

a. Care should be taken not to discuss sensitive matters in the presence of other people; consequently such conversations should not take place in open plan offices.

b. Additional restrictions apply to telephone conversations. These are detailed in Chapter 9.

Siting of Electronic Office Equipment

05242. In open plan offices the siting and supervision of computer printers, faxes and photocopiers is important. The following rules apply:

a. Computer printers are to be sited either adjacent to an individual's desk if connected to a stand-alone computer, or within a group area if connected to a networked system.

b. Faxes and photocopiers are to be under the direct control of their nominated supervisors.

c. Existing departmental security regulations are to apply.

Duty Security Checker

05243. Open plan offices are to employ a duty security checker system to ensure that all protectively marked material is secured at cease work. Alternatively, defined working group areas within the open plan offices can ensure that the last person leaving each area conducts a security check. This check should be certified on a check list which clearly indicates the extent of the area to be checked.

Key Security

05244. Within open plan offices the reduction in suitable wall space restricts the use of combination key boxes for the secure storage of keys. Key security arrangements are to be reviewed to ensure that an effective system is established utilising security containers and taking account of the requirements of authorised late workers.

Visitors

05245. Open plan offices make it more difficult to control the movement of visitors and contractors e.g. maintenance staff. Uncleared personnel are always to be escorted. Cleared personnel do not require escorts and staff should be alert to unknown personnel in their work areas. Strangers should be challenged.

Security Measures Checklist

05246. The following is a list of points to be covered when planning security measures in an open plan environment.

a. Identify those groups dealing with similar subjects and with similar access to protectively marked material and try and ensure they are adjacent to each other.

b. Arrange for the more sensitive material to be compartmentalised, where there is justification, or to be furthest from points of general access to prevent overhearing or overlooking of material by unauthorised personnel.

c. Define boundaries of small working groups. The boundaries are to be used for determining supervision and cease work close down procedures. These procedures should be recorded.

d. Within these groups consider the arrangements for controlling protectively marked material, security containers, PC's and terminals, printers, photocopiers and faxes.

e. Ensure staff are aware of their responsibilities, and the need for care when handling or discussing sensitive matters in an open plan environment.

f. Check that a suitable system exists for securing protectively marked material and keys at cease work.

g. Establish either a last man out system for working areas or a duty security checker system to ensure the security of areas at the close of work.

h. Ensure that the last man out or duty security checker is aware of the checks to be conducted and form to be completed.

Security of Documents and Activated IT Systems in Unattended Offices

05247. Protectively marked documents must be secured in appropriate security containers when offices and rooms are vacant. Security Authorities may waive this requirement, where appropriate, only during normal working hours where the room or compartment is fitted with a lock (including digital push button locks), the key or combination to which has always been controlled as a security key or combination, and the following conditions apply (comparable rules apply to IT systems which are activated, see Volume 3 Chapter 2):

a. **Periods of time.** The maximum lengths of time that documents may be left unattended in locked offices are:

(1) TOP SECRET - 30 minutes.

(2) SECRET and CONFIDENTIAL - 4 hours.

(3) RESTRICTED - 8 hours.

Note: Special Handling material will continue to be subject to specific guidance issued by originators.

b. **Security requirements.** The following security requirements are to be applied for all protectively marked documents left in unattended offices, except for RESTRICTED documents when only the requirements of Sub-paras (1) to (3) inclusive apply:

(1) All windows, doors and other means of entry to the vacated office are to be secured. Where doors have 2 means of locking (eg digital push button lock and normal key lock) and the absence is in excess of 30 minutes, both means of locking should be utilised (2 means of locking need not be utilised for RESTRICTED documents).

(2) It must not be possible to view documents (including computer screens) from a window, glass door or any other means such that it is possible to identify the protective marking of the document or view its contents (including by the use of image intensifying or photographic equipment).

(3) The key to the door is to be held by the office occupant at all times except when it is deposited with an authorised holder.

(4) Other personnel must occupy the building at all times.

(5) There must be control of entry to the building, establishment or unit.

(6) The period of absence is not to be a matter of regular routine or predictable pattern (absences over the lunch period need not necessarily be included here, provided that the Security Authority is satisfied that the overall security measures are adequate).

05248. Separate rules exist for open plan offices (see paras 05234-05246).

ANNEX A TO SECTION II

SPECIAL SERVICES GROUP (SSG)

General

1. The purpose of this Annex is to describe the role of SSG in supplying services to MOD, and the arrangements for funding and the control of funding those services. SSG provides in-Government expertise in most aspects of physical security for employment by MOD. In setting its charges, SSG will minimize costs but is under HM Treasury remit to achieve full recovery.

2. SSG is organised into two separate parts:

   a. The SSG Authority, providing an advisory service.

   b. The SSG Executive, providing a security implementation service.

3. The services that SSG provide for the MOD are described in a Supply and Services Agreement (SSA). MOD sponsors are as follows:

   a. SSG Authority SSA – the point of contact is DD Def Sy(Phys).

   b. SSG Executive SSA - the point of contact is DE Contracts

SSG Authority

4. The SSG Authority provides an **advisory** service that is currently free to MOD customers at the point of delivery. Application for this service is to be made through and supported by, PSyAs using the request form at Annex F. Tasking of the SSG Authority is to be restricted to seeking advice on technical aspects that are beyond the scope of available in-house security expertise. Examples are those services detailed at sub-paras 7a and 7b. Wherever possible, the costs of security advice for major projects, future major projects and the services described in sub-paras 7c, d and e should be included within the budget of the project.

5. Where the SSG Executive are contracted to carry out the work, security advice for the work, and any costs incurred, will be on a repayment basis and charged to the contract.

Funding Management for SSG Authority Work for MOD

6. Under the terms of the SSA, SSG will send a monthly invoice to D Def Sy for payment, for completed SSG Authority services. A copy of the invoice will be sent by SSG to each PSyA. It is the PSyAs responsibility, within one month of receipt of each monthly invoice, to advise D Def Sy in writing if invoiced work has not been satisfactorily completed. In the event of a dispute over a service provided by the SSG Authority, resolution will be carried out under normal works service procedures.

SSG Authority Services

7. The SSG Authority will provide, on request (and in accordance with given timescales), the following services:

a. A security survey report describing the overall security strategy with outline proposals (a brief), quantified performance standards and parameters and an order of cost estimate.

b. An independent evaluation of the detailed design to ensure that the security requirement has been met.

c. Expertise in testing or observation of tests on behalf of the PS or PROM as appropriate.

d. A 'troubleshooting' service to examine and report on specific problems with installed security systems and equipment.

e. Maintenance of security equipment database and trials reports.

SSG Executive

8. The SSG Executive can be employed by PSs/PROMs either in competition with commercial firms or where the Security Authority has directed that SSG should be used; PSs/PROMs should note the following:

a. Where it has been so directed, PSs and PROMs should ensure that SSG's responsibilities are defined within the management system of the works in general and are consistent with any regulations. Specifications and documentation should be similar to those under which contractors or sub-contractors are retained using WSMs or PMs.

b. The management of services carried out by the SSG Executive and its construction, design and management regulation aspects, should be defined in the PM's contract documents for projects or in the order placed on the WSM for PROPMAN work.

c. All aspects of SSG Executive service for MOD will normally be carried out on a repayment basis, including advice given by the Executive.

ANNEX B TO SECTION II

SECURITY ADVICE - CAPITAL WORKS PROJECTS

STAGE 1

Statement of Requirement (SOR)

ESyO as stakeholder, to formulate SSR element of SOR, taking advice if appropriate, from Sector Security Authorities or other specialist security staffs. SSR to include, as a minimum:

1. Vulnerability of Project facility to threats (high/medium/low).

2. Identify what is being protected.

3. Possible alternatives which would reduce security requirement (eg could protectively marked material be stored elsewhere?)

As much detail as possible should be provided to identify security implications. Further advice on drafting the SSR can be found at Annex E.

STAGE 2

SOR Staffing

PSyA to note and comment on content of SOR. PSyA to commence formulating checklist of security needs in order to inform the Options Study.

STAGE 3

Option Study (OS)
Preparation/Staffing of draft OS

PSyA to provide a detailed check-list of security requirements for each option under consideration (for example: robustness, glazing, locks, fencing, IDS and lighting standards). As much detail as possible should be provided in order to ensure that all appropriate security measures are incorporated and subsequent OS costings are

accurate. To assist with this process it may be appropriate for the ESyO to start developing the OR seeking assistance from specialist security staffs (in exceptional circumstances the PSyA can request assistance from SSG). Further advice on the drafting of the OR can be found at Annex E.

STAGE 4

OS

STAGE 5

Approval by Budget Holder

ESyO to attend Siting Board (Siting Board may have been convened earlier). Any further comments on security requirements to be passed to PS and PSyA.

STAGE 6

Project Brief (PB) Preparation

1. The PB is the basis on which the appointment of the commercial Project Manager (PM) is made.

2. As required, PSyA attends Project stakeholders meeting.

3. PSyA decides whether further specialist security input is required (eg by specialist security staffs or SSG).

4. PSyA oversees preparation and completion of detailed OR (further advice on the drafting of the OR can be found at Annex E)).

Note: It is important to ensure that the security scope of work in the PB is fully defined. It should include only the essential security features (to MMR)* which must be incorporated within the Project. Any changes to the scope of work after the appointment of the Project Manager will not be affordable.

* In this context, MMR means only those measures which are necessary to meet operational or other military need.

STAGE 7

Appointment of Project Manager

STAGE 8

Preparation of Design Brief

PSyA:

1. Attends design meetings as required.

2. Maintains a constant dialogue with Project Sponsor (PS) during design development to ensure that scope of security work identified in the PB is being properly interpreted.

STAGE 9

Design

PSyA approves final design.

STAGE 10

Appointment of Contractor

STAGE 11

Construction

STAGE 12

Hand-Over

ESyO attends Pre-Acceptance Board Testing and Handover Boards. PSyA attends (if required). Certificates of acceptance to be provided to PS.

This page intentionally blank.

ANNEX C TO SECTION II

SECURITY ADVICE - WORKS SERVICES (PROPMAN)

STAGE 1

Works Request

ESyO should routinely comment on new works proposals. He is to provide an OR, taking advice, if appropriate, from PSyA or other specialist security staffs and attend siting boards (further advice on drafting the OR can be found at Annex E).

STAGE 2

Maintenance of the

Forward Maintenance Register

ESyO to ensure Property Manager (PROM) includes security-related works and takes account of need to replace CCTV, IDS etc in future years.

STAGE 3

Annual LTC Process

PSyA to provide advice to TLB work staffs during the validation process.

STAGE 4

Approval by Budget Holder (Work listed in Pre-planned

Maintenance Programme)

ESyO to attend siting board. TLB specialist to comment upon Forms 2.

STAGE 5

Design

ESyO to review Work Service Manager (WSM) sketch plans and working drawings.

STAGE 6

Construction Phase

ESyO to implement necessary vetting procedures if appropriate.

STAGE 7

Completion of Works

ESyO attends Pre-Acceptance Board Testing and handover boards. Certificates of acceptance to be provided to the PROM.

ANNEX D TO SECTION II

SECURITY INVOLVEMENT IN WORKS RELATED PRIVATE FINANCE INITIATIVE

To be issued.

This page intentionally left blank.

ANNEX E TO SECTION II

DRAFTING THE STATEMENT OF SECURITY REQUIREMENT (SSR) AND OPERATIONAL REQUIREMENT (OR)

Statement of Security Requirement

1. The SSR (also known as a brief or high level OR) forms part of the work service SOR. It is a high level statement which indicates the assets to be protected, the threat assessment, the perceived vulnerabilities to the threat, the security level required, and the reliability and availability required of any proposed systems. The SSR is developed by the ESyO, in consultation with the PSyA, when a security requirement has been identified. The PROM/PS provides (via the ESyO) the Security Authority with the basis against which the threat and security concept is set. The threat appreciation is to incorporate any relevant local factors; eg a risk assessment of the site and a summary of possible methods of attack.

Operational Requirements for Security Measures

General

2. An OR is a statement of needs based on a thorough and systematic assessment of the problems to be solved and the hoped for solutions. The important thing to remember is that the OR will be used to guide the eventual design process for any recommended security measures. It must be clear as to what is required so that there are no surprises in the future; any changes after contract-let may not be affordable. The OR will outline in some detail the requirements in terms of deterrence, detection, physical delay, surveillance and response. The OR is the critical document that provides the link between the high level need and the system procurement process. Every step on the road to an installed system should be directed at achieving the OR. Without an OR the performance criteria cannot be agreed; without performance criteria it will be difficult to reliably test and commission the completed installation and there will be no mechanism for rejection of an inadequate system.

3. SSG have produced, on behalf of EDICTS, a guide to producing ORs for protective security measures. Copies of the document can be obtained from TLB PSyA staffs. The methodology of the checklist is summarised below:

a. **Content of the OR.** The following list is the realistic minimum of points that must be addressed in the OR:

(1) Assets to be protected.

(2) The threat.

(3) Consequences of compromise.

(4) Probability and frequency of occurrence.

(5) Level of security required - based on the classes in Section I.

(6) Areas of concern.

(7) Function of any proposed measures.

(8) Environmental conditions expected.

(9) Success criteria.

In addition it is useful to include:

(10) Responses.

(11) Information transmission.

(12) Information handling.

(13) Operators tasks.

(14) Training needs.

b. **Producing the OR.** Using the SOR (incorporating the SSR), the OR is written by the ESyO with assistance, if necessary from the TLB PSyA staffs, a facilitator (such as SSG) and other stakeholders. There must be communication with ALL the stakeholders during the production of the OR. The stakeholders are everyone who has an interest in the operational security of the site or building. This includes security managers, building owners, building user representatives, budget holders, and the operators of any technical security systems, current or proposed. There are 5 steps to be followed in producing the OR:

(1) **Step 1.** Agree and list the assets and physical areas of concern.

(2) **Step 2.** Complete the OR checklist.

(3) **Step 3.** Produce a checklist summary.

(4) **Step 4.** Consider possible solutions.

(5) **Step 5.** Write the OR statement.

ANNEX F TO SECTION II

RESTRICTED

(When completed)

REQUEST FOR INITIAL SSG ADVISORY SERVICE - SECURITY REQUIREMENTS AT A DEFENCE SITE

(SECTIONS 1, 2, 3, 5, 6 TO BE COMPLETED BY ORIGINATING UNIT AND FORWARDED TO SECTOR SECURITY AUTHORITY (SSA). SECTION 4 (APPROVAL) TO BE COMPLETED BY SSA AND FORWARDED TO SSG (COPIED TO DDEF SY)

File Reference :

From: eg. DNSyICP / HQ Land / HQ STC / CB Sy / DLO / DPA

To : Head of Branch, Room 9/42, Special Services Group, SSG, St Christopher House, Southwark Street, London SE1 OTE. *(Fax No: 0207 921 3802)*

Copy to: DDef Sy-Phys(Tech) (Fax No: 0207 218 3993)

References (See Note 1):

Section 1 - Location of Site

Grid reference :

Postal address :

Type of site: urban/rural, shared/sole occupant.

Type of work (See Note 2): new build/ refurbishment/ IDS/ PIDS/ CCTV/ AACS/ SAMS/ lighting/ building construction/ fences/ blast protectio

RESTRICTED

(When Completed)

Area of advice (See Note 3): option study/ pre-project advice/ initial project advice/ audit established system/ audit newly installed system/ trouble shooting/ other (please specify).

Section 2 - Primary Establishment

Title :

Role :

Security category of establishment:

Highest level of protection: TOP SECRET / SECRET / CONFIDENTIAL / RESTRICTED

POINT OF CONTACT

Name:

Appointment:

BT Tel No: **BT UNCLAS Fax No (See Note 4):**

Section 3 - Security Section/Unit

POINT OF CONTACT

Name:

Appointment:

BT Tel No: **BT UNCLAS Fax No:**

RESTRICTED

(When Completed)

RESTRICTED

(When Completed)

Section 4 – Approval from TLB PSyA Staffs

POINT OF CONTACT

Name :

Appointment:

BT Tel No: **BT UNCLAS Fax No:**

Section 5 – Advisory Input Requirements

Timsecale (See Note 5):

Contacts (See Note 6):

Distribution for SSG Advisory Report

Name:

Appointment:

Address:

No. of copies:

BT Tel No: **BT UNCLAS Fax No:**

Section 6 – Work Services Information

The following items are attached for information (See Note 7)

Operational Requirement: Yes/ No

Threat/ Risk Assessment: Yes/ No

RESTRICTED

(When Completed)

RESTRICTED

(When Completed)

Other Plans and Documentation (please specify):

Distribution:

External:

Action (See Note 8):

Information (See Note 9):

Notes:

(1) References as necessary e.g. G2 HQ LAND Control No.

(2) Description of problem/ project/ area of advice/ work required.

(3) The following services cannot be obtained through the D Def Sy funded SSG Advisory Account: installation, maintenance, commissioning, detailed project advice, purchase of equipment, examining tenders. If in doubt, speak to your PSyA Staffs or DDef Sy-Phys(Tech).

(4) SSG Burtonwood is not connected to the Military Telephone Network.

(5) Start/ end dates, particular dates to note i.e. meetings.

(6) Initial point of contact for SSG Adviser to discuss work service particulars or arrange site visit.

(7) As Operational Requirement and Threat/ Risk assessment should be attached to this request form. If not, then an explanation should be given as to why these documents have not been generated. Plans of the site/ establishment/ building (preferably A3 size) will be of assistance to SSG in completing their report.

(8) Request form to be forwarded to relevant PSyA Staffs for action unless command instructions in place that state otherwise.

(9) Complete as appropriate e.g. HQ G2/G4, Area Sy Team, P&SS Unit, MI Bn DLO/DPA Sy Staff etc

RESTRICTED

(When Completed)

ANNEX G TO SECTION II

COUNTER TERRORIST PHYSICAL SECURITY MEASURES FOR ALL MOD OWNED OR OCCUPIED BUILDINGS

Introduction

1. This Annex details the minimum counter-terrorist physical security measures which are to be applied to all MOD owned or occupied buildings.

2. The physical security measures, adapted for the MOD, are based on Cabinet Office guidelines on robustness measures for buildings. The purpose of these measures is to limit damage to the building fabric and injury to the occupants, whatever the level of threat. Given the varying function and location of MOD buildings, physical security measures should be applied on the basis of vulnerability of the site.

3. It is the responsibility of PSyAs to ensure that the measures applied are appropriate. Accordingly, ESyOs and/or PSyAs, in consultation with DE SCG, TLB works advisers and the Project Sponsor or Property Manager, are to assess the vulnerability of buildings as either HIGH, MODERATE or LOW taking into account the following:

a. Location ie whether or not the building is within a secure perimeter.

b. Perimeter security and access by the public.

c. The building aspect in relation to the perimeter.

d. The protection afforded by other buildings, other features and/or landscaping.

e. Whether or not the building is normally occupied.

f. Building usage e.g. housing departments involved in the fight against terrorism.

4. When determining building vulnerability, due account should be taken of the following **general** rules (together with the considerations at sub-paras 3b to f above):

a. Buildings that are not located within a secure perimeter or are located within 100 metres of a secure perimeter will be HIGH unless other factors afford protection from bombs/mortars.

b. Buildings that are normally occupied by personnel, are located beyond 100 metres within a secure perimeter, will be MODERATE unless other factors afford protection from bombs/mortars.

c. Buildings that are not normally occupied by personnel will be LOW.

5. The physical security measures fall into two distinct categories:

a. **Standard measures.** Those measures that cannot be applied or removed quickly in line with a changing threat. There are two sections of Standard Measures, those for new construction and those for existing construction; and

b. **Enhanced measures.** Those measures which can be applied or removed as the threat changes. It is important to carry out a security survey to establish the appropriate Enhanced Measures which are to be included in any contingency plan.

Standard Measures

6. These measures are to be applied to all new MOD buildings being constructed, leased for MOD use or refurbished. When applying these measures, PSyAs should exercise common sense and give consideration to omitting certain standards in the case of buildings deep within the perimeter or with low occupancy, domestic facilities such as housing and sporting facilities such as squash courts.

a. **SM.1 - Construction Standard**

(1) The building should be of framed construction using either structural steel or **in situ** reinforced concrete.

(2) The structural frames should be designed to the "degree of robustness" required by the relevant British Standards, whatever the number of storeys (ie all buildings less than 5 storeys high should be designed as a 5 storey building for robustness only).

(3) If structural steelwork is used, the beam/column connections are to be designed to carry load reversals and where possible the facade columns and beams should be concrete encased.

(4) The floors and roof slabs should be constructed with **in situ** reinforced concrete, or with pre-cast concrete slabs with a structural topping suitably tied into the structural frame.

(5) Cladding should be either pre-cast concrete panels or solid masonry. If pre-cast systems are used the fixings of the panel back to the structure are to be robust, easily accessible and repairable. Further the cladding system should be designed so that each panel may be removed without affecting the surrounding panels.

b. **SM.2 - Bomb shelter area (BSA) accommodation**

(1) **High vulnerability.** BSA accommodation should be provided and must be sufficient for the maximum number of people likely to be occupying the building. BSA provision may be achieved by careful planning of cores constructed in reinforced concrete, or by robust basement construction.

(2) **Moderate vulnerability.** BSA accommodation may be provided for people likely to be vulnerable. An alternative of emergency evacuation planning may be preferred.

(3) **Low vulnerability.** An emergency evacuation plan is to be in place.

c. **SM.3 - Glazing protection.** Glazing protection minimises the injuries to personnel and damage to assets by reducing the quantities of flying glass.

(1) **High vulnerability.** This protection is achieved by the installation of laminated glass in frames which are securely fixed to the surrounding structure. The plastic interlayers within the laminated glass must be polyvinyl butyral (pvb) for the glazing to offer blast resistance. If a better level of protection is required, then 7.5mm laminated glass in purpose designed frames should be specified. If a double glazing system is to be used, then the outer leaf should be 6mm toughened glass of the appropriate thickness to suit the standard design requirements; and the inner pane should be 6.8mm laminated glass for standard frames or 7.5mm thick laminated glass in enhanced frames.

(2) **Moderate vulnerability.** If single glazing is specified, then the laminated glass should be a minimum of 6.8mm thick in standard frames.

(3) **Low vulnerability.** As above or consideration should be given to the use of anti-shatter film.

d. **SM.4 - Access control.** A good access control system should be installed at all pedestrian and vehicular entrances; this will minimise the opportunity for the deployment of a device within the building. A device placed inside a building would cause greater damage and potentially more injuries that a similar sized device deployed outside the building.

e. **SM.5 - Counter terrorist contingency plan.** Current Health and Safety legislation requires an employer to have established appropriate procedures to be followed in the event of serious or imminent danger. Actions to be taken in the event of an attack are given in Chapter 7.

f. **SM.6 - X-Ray Screening of delivered items.** Where X-ray screening of mail and delivered items is to be carried out, a purpose designed room should be constructed so as to minimise the consequences of an explosion and offer a degree of protection to operators and staff.

7. For buildings currently occupied.

a. **SM.1 - Construction standard.** Any of the measures noted in SM.1 for new construction which are provided by the existing structure will minimise the consequences of an explosive device.

b. **SM.2 - Bomb shelter area (BSA) accommodation.** If the building is of framed construction it may offer BSA accommodation. Structural engineering advice should be sought to ensure that the building construction is suitable and the Shelter Area construction meets current guidance. If the building is not framed or does not provide suitable BSA accommodation, external evacuation will be required as part of the contingency planning from the threat of explosive devices.

c. **SM.3 - Glazing protection.** Where the glazing is being renewed or refurbished consideration should be given to replacing the glazing in accordance with the recommendations in SM.3 for new construction. In all other cases anti shatter film (ASF) should be fitted in the internal surface of all external glazing, whatever the height of the building. Bomb blast net curtains (BBNC) may be fitted where appropriate. In the case of timber framed 'Georgian' windows ASF and BBNC should be fitted.

d. **SM.4 - Access control.** See SM.4 for new construction.

e. **SM.5 - Counter terrorist contingency plan.** See SM.5 above for new construction.

f. **SM.6 - X-Ray screening of delivered items.** See SM.6 above for new construction.

Enhanced Measures

8. Enhanced measures are those measures that are to be implemented, or removed, as the Alert States increase, or decrease.

9. Each Alert State requires a certain set of measures to be implemented. A comprehensive set of measures for each of the Alert States is to be incorporated into the contingency plan.

10. Not all the measures will necessarily be appropriate for a particular establishment. It is, however, important to undertake a Security Survey examining such aspects as location, exposure, activity, site conditions, etc so as to identify those measures that are appropriate and then incorporate them into the contingency.

SECTION III TO CHAPTER 5

EXTERNAL PERIMETER SECURITY MEASURES

Introduction

Perimeters

05301. A perimeter may be defined by a natural boundary, by free-standing fences or walls, by the outer walls of a building or by divisions within it. Its function is to provide a degree of physical, psychological or legal deterrence to intrusion. Its effectiveness as a security measure can be enhanced by the deployment of perimeter intruder detection systems (PIDS), closed circuit television (CCTV), security lighting and guard forces.

Further Information, Advice and Guidance

05302. Further information and direction on perimeter security measures can be obtained from the following sources:

a. Where establishments are considering the installation of perimeter security measures Command security staff are to be consulted to provide specialist advice and any appropriate policy input; Section II to this Chapter provides information and direction on the procurement of major security equipments and systems. In addition, where such work constitutes a works service project, the procedures detailed in Chapter 5, Section II, Annex A are to be adhered to.

b. The PIDS 'Family of Documents' (full title; 'Family of Documents to Establish Optimum External Security Systems - Volume 3 - Perimeter Intruder Detection Systems (Ref 94066)) produced by the Security Equipment Assessment laboratory, under the auspices of EDICTS provides detailed advice, guidance and instruction on the deployment of PIDS. The document is the authoritative publication for the use by MOD establishments.

Fences

General

05303. A perimeter fence forms a barrier and identifies the boundary of a protected or restricted area. The level of protection offered by a fence depends on:

a. The height of the fence.

b. The construction of the fence.

c. The material used in the fence.

d. Any additional security features used to increase its performance or effectiveness such as topping, PIDS, lighting or CCTV.

The type of fence used on the perimeter of a site is to reflect the type of threat, i.e. terrorist, criminal etc.

Purpose of Fences

05304. Fences are not always to be regarded as being a major obstacle in themselves. They are primarily a means of:

a. Delineating a boundary/area hence protecting against casual intruders.

b. Channelling visitors to legal points of entry.

c. Deterring and delaying unlawful intruders who are normally loathe to operate with an obstacle behind them, particularly if they have no guarantee of getting back to their point of entry.

d. Assisting guard patrols and easing the employment of guard dogs.

Effectiveness of a Fence

05305. The effectiveness of a fence as a barrier to or deterrent against intruders can be increased by the following:

a. Surveillance of the fence by members of the guard force.

b. The alarming of the fence with some form of PIDS.

c. The addition to fences of suitable security lighting.

d. Ensuring that fences are inspected frequently to ensure that they are in good condition, have not been tampered with and that they and the immediate area are clear of vegetation.

Classes of Fences

05306. The Classes of fences are at para 05124 and the types of specific barriers that fall into each Class are shown at Section I, Annex E.

Working and Operational Areas

05307. Ideally, a fence should enclose the entire working or appropriate operational areas within an establishment. When this is not practicable, individual key areas are to be enclosed where possible. Careful planning will ensure that such installations are grouped together and subjected to coordinated security control. The aim is to draw as tight a ring as possible around the key area and to apply the main security effort there.

Outline Specification for Fences

05308. The following design features for security fences apply:

a. **Height and construction.** The height and construction of a security fence is to be commensurate with the degree of physical deterrence required. Defence Estates (DE) has details of the approved types of fence. Of these, the current minimum Defence Standard is the 1.80m high barrier fence (DE SD50/1-5). However, this type of fence should be replaced by a 2.4m security fence, BS 1722 Part 101990 (Weldmesh), during refurbishment or on life expiry of the barrier fence. In some establishments existing fences or walls of the buildings themselves and/or pallisade fencing may provide a similar degree of protection. Whenever toppings on a 1.80m high need to be replaced, the advice of DE should be sought.

b. **Access through the fence.** Access is not to be possible under the fence, or through drains and culverts beneath it. Points such as drains and culverts should be identified as weak points and due for special attention.

c. **Line of fence.** The following considerations are to be taken into account in regard to the line of fences:

(1) The fence is to, wherever possible, run in straight lines for ease of surveillance and erection.

(2) Junctions where the fence changes direction are usually easier to climb and are therefore be kept to a minimum.

(3) Advantage is to be taken of existing or natural features so as to increase the protective value of the fence.

(4) Using natural or existing features may help minimise the use of material in the fence.

(5) The manpower that will be needed for the surveillance of the fence.

d. **Siting of fences.** A Security/Barrier fence should be sited around vulnerable areas to permit economic patrolling or surveillance. However it should be built at least 25m away from any work, Mess or accommodation block, where possible, to provide protection against an explosive device being placed against the fence or a satchel type IED being thrown over the fence to reach the buildings. Where possible, ground on both sides of the fence is to be cleared to remove cover for potential intruders. Therefore, the fence should, if possible, be at least 10m back from the marked boundary of MOD land. This will facilitate the creation of a sterile zone, both to allow the installation of certain types of PIDS and also to allow space for lighting and cameras to cover the fence face and the approaches to it, if the use of

PIDS is envisaged. Careful planning and the selection of the best line for the fence using natural features will increase the protective value of the fence, and minimise the use of material and manpower required for construction and subsequent security coverage. Where a security area abuts an external boundary, additional security measures should also be considered and applied.

e. **Visibility.** Wherever possible, the whole of the fence area is to be visible to resident or patrolling guards. The perimeter can be shortened in places to avoid pockets in the fenced area which would otherwise be out of sight. Closed circuit television (CCTV) may also help to improve visibility at particular establishments. JSP 436 Chapters 3 and 10 provide more information on fence surveillance.

f. **Anti-climbing devices.** Anti-climbing devices such as barbed wire or barbed tape concertinas are to be used at the top of the fence. A barbed wire or barbed tape concertina laid inside the fence at its base can discourage burrowing; JSP 436 Chapter 3 provides diagrams of such devices. As there may be legal implications where such devices are used in areas to which the public have access, advice on the matter is to be sought from Command security staff.

g. **Gates.** The following measures apply to gates:

(1) Gates are to be of comparable standard to the fence.

(2) The number of gates is to be reduced to a minimum.

(3) Locking is to be achieved by padlock and locking bar being welded to the gate and frame, or to both leaves of a double gate.

(4) The bottom of gates are not to have a ground clearance in excess of 50 mm.

(5) Unmanned gates are to be kept locked with approved padlocks, included in patrol beats and inspected regularly.

(6) Manned gates are to have adequate communications to Guardroom or Central Security Control.

h. **Compatibility.** Fences are to be compatible with the terrain and with any requirement for IDS and/or for CCTV.

Types of Fence

05309. Transparent fences should normally be preferred to opaque fences where there is a need for guards to see outside the protected area. They are to be constructed of the following:

a. Welded mesh.

b. Steel palisades.

c. Expanded metal (XPM).

d. Chain link.

Detailed specifications can be obtained from SSG via Command security staff.

Opaque Fences

05310. Where an opaque fence is needed the following applies:

e. **Steel profile fences.** Steel profile fences are generally recommended. They are made of galvanised steel sheets bolted to the framework of a steel fence.

f. **Walls.** Walls are not usually recommended for security purposes because, although comparatively difficult to penetrate, they are expensive to

construct. However there will be occasions where walls are essential for a specific requirement that has to be met. Advice from Command security staff is to be sought by establishments in such circumstances.

g. **Wood fencing.** Wood fencing of any kind is comparatively weak and not recommended for security use other than for screening purposes.

Selection of grade of fence for a site.

05311. The selection (and therefore the expenditure required) of a particular Class of fence for a site must be justified in relation to the threat that an establishment faces or is expected to face taking into account a risk assessment of the site. Establishments are to consult Command security staff prior to a major procurement of fencing.

Entrances and Exits

05312. Heads of establishment are to designate points of entry and exit to/from their establishment and promulgate conditions concerning their use in establishment standing orders (security). Such entrances and exits are to be kept to a minimum although at least one alternative entrance/exit must be able to be used when required. Further instructions for control of entry are at Section IX of this Chapter; additional guidance is in Chapters 3, 5 and 10 of JSP 436.

Security Notice Boards

05313. Prohibited Place notices are to be displayed on operational sites at official points of entry, such as gates or access roads, whereas playing fields, married quarter estates etc are to have signs reading 'MOD Property. Keep Out'. Prohibited Place Notices are to be worded as follows:

THIS IS A PROHIBITED PLACE WITHIN THE MEANING OF THE OFFICIAL SECRETS ACTS - UNAUTHORIZED PERSONS ENTERING THE AREA MAY BE ARRESTED AND PROSECUTED.

05314. Except for notices indicating that police/military working dogs are on patrol, those indicating MOD property, Official Secrets Acts notices and those instructing visitors to report to the Guardroom/Control of Entry Point. Security notice boards are not to be used to indicate boundaries or perimeters.

Units Overseas

05315. Overseas units are to follow the spirit of para 05313, tailoring the notice to the requirements of local law and of Status of Forces agreements.

Perimeter Intruder Detection Systems (PIDS)

Definition

05316. PIDS are electronic devices for detecting the entry or attempted entry of an intruder across the external perimeter of an installation and signalling an alarm.

Use of PIDS

05317. In securing assets requiring a high level of protection, the use of PIDS can be considered. They can usefully enhance the effectiveness of other perimeter defences (such as fences and guard forces) but they are prone to false alarms (which need to be verified by CCTV or a guard force) and, if unsuitably sited, their probable rate of detection may be low. See para 05302 for information on the PIDS 'Family of Documents'.

Operational Requirement

05318. PIDS are expensive and care is to be taken in the selection, application and installation of a PIDS to prevent it being circumvented or its usefulness being impaired by a high incidence of technical problems or false alarms. An Operational Requirement (OR) is to be compiled by the establishment after consultation with and approval by Command security staff. Establishments are to define clearly what they expect of a PIDS and to be aware of its limitations. In setting the requirements for a PIDS installation the following is to be specified:

a. The area/equipment to be protected.

b. Any special requirements affecting the areas concerned and the degree of security protection necessary.

c. Whether linkage to other electronic systems such as CCTV or AACS is required.

d. The overall security plan and details of all related measures relevant to the design of the system.

e. The type of reaction force or monitoring arrangements required.

f. The position of the alarm display panel and details of related security procedures.

Site Survey

05319. Following approval of the OR, a site survey is to be arranged by Command security staff (who may task their single-Service security organisation, or SSG. The site survey is to consider:

a. The type of fence or wall requiring coverage.

b. The length of each perimeter requiring coverage.

c. Whether there is sufficient ground available to establish sterile detection zones (if appropriate) on the attack side of each perimeter.

d. Local soil and ground surface conditions.

e. Prevailing weather and local wild life.

f. The resources, including CCTV and guards, available for alarm verification.

See also Chapter 5, Section II, Annex A for co-ordination of security aspects of works services.

System Audit

05320. An audit of the PIDS system is to be carried out by professional security staff.

System Maintenance

05321. To ensure any system continues to provide its optimum performance, performance testing, servicing and preventative maintenance is needed. These tasks should keep costs down and maintain acceptable performance. The frequency for carrying out each task should have been determined after consideration of the possible threat, the manufacturer's recommendations, the technical requirements of the equipment, the effort required to complete each task and the cost of carrying out the task compared to the benefits to be gained. Because PIDS consist of electronic devices operating in an outdoor environment system confidence and availability can only be maintained through regular maintenance, it is therefore recommended that systems receive at least 4 maintenance visits per year.

Security Lighting

Effective Use of Lighting

05322. Lighting can make an important contribution to physical security but to be effective it should be used in association with guards. If incorrectly applied, it can assist intruders more than guard forces. Security lighting is to:

a. Allow guards to see intruders before they reach their objectives.

b. Conceal the guards from intruders.

c. Deter intruders or hinder them in their purpose.

05323. Security lighting acts as a particularly good low cost deterrent. Even a low level of illumination can deter potential intruders. Lamps which require long warm-up periods are unsuitable for certain security lighting applications. Time switches, movement sensors or photo-electric sensors can be useful for the control of security lighting, but the latter are vulnerable to deliberate interference.

Types of Security Lighting

05324. The following types of security lighting meet particular applications:

a. **Perimeter lighting.** Perimeter lighting is to be designed to cast a uniform light on the perimeter. This is to be provided by overhead lamps or by low mounted lamps which will create a glare effect to dazzle and deter intruders. If the latter are used, they are not to create a nuisance or hazard outside the perimeter. The lighting is to be so designed so that it does not reveal the position of patrolling guards. Brightly lit guard posts or reception rooms where the guards are clearly visible or silhouetted are to be avoided.

b. **Area lighting.** Area lighting is to illuminate areas inside the perimeter which intruders must cross in order to reach their objectives. The following measures apply:

(1) Area lighting increases the guards' ability to detect intruders and acts as a powerful deterrent.

(2) The illumination is to be even and without shadows.

(3) Every part of each area to be illuminated is to be lit by at least two lights to guard against lamp failure.

c. **Local lighting.** Local lighting illuminates areas inadequately covered by area lighting and which could conceal an intruder. The following applies:

(1) Small bulkhead lights, tough and resistant to interference, are preferred.

(2) Fluorescent or tungsten-halogen lamps can be used as miniature flood-lights.

(3) All dark spots are to be eliminated.

(4) Roofs, fire escapes and emergency exits should be illuminated by such local lighting.

d. **Flood lighting.** Flood lighting may be used to illuminate surfaces (eg buildings and fences) which intruders must pass in front of to reach their objectives. The following applies:

(1) At the low illumination levels typical of security lighting the eyes rely mainly on ability to recognise outline shapes.

(2) As a moving silhouette can readily be seen against an illuminated/light coloured wall, buildings can be painted white or some other light colour.

Physical Protection of Lighting Installations

05325. The physical protection afforded to lighting installations is to be related to the threat. The following measures apply:

a. The fitment of robust fittings, armoured cables and protected switch-gear where appropriate to the threat.

b. The electrical supply is to be separated from that of the normal power supply.

c. There is to be a standby electrical supply with auto start and changeover in the event of mains failure.

d. Lighting circuits to be linked with intruder detection systems so that tampering sets off an alarm.

This page intentionally left blank

SECTION IV TO CHAPTER 5

THE PHYSICAL SECURITY OF BUILDINGS

General

Further Advice on Threats and Counter Measures

05401. Advice on the current threats and specialist countermeasures can be obtained from the following sources:

a. **Espionage/terrorist threats and their counter measures.** For espionage/terrorist threats and their counter measures the following sources are available:

(1) Advice on both surreptitious and terrorist threats can be obtained from PSyAs who are advised of current threats by D Def Sy.

(2) Advice on structures, building materials, window and door design, grilles and glazing materials etc, required to counter them can be obtained from PSyAs who may consult MOD Defence Estates (DE) Specialist Services as necessary.

b. **Criminal threat and counter measures.** Advice on local criminal threats may be obtained from the crime prevention officer and the architectural liaison officer of the local civil police force via the Service police/MDP. Some Service police units also have architectural liaison officers.

c. **Works services**. Where establishments are considering the installation of physical security measures, PSyAs are to be consulted to provide specialist advice and any appropriate policy input. In addition, where such work constitutes a works service project, the procedures detailed in Chapter 5, Section II, Annex A are to be adhered to.

d. DE Specialist Construction Functional Standard - Glazing Standards for MOD Buildings subject to Terrorist Threat.

e. DE Specialist Construction Design Guide - Robustness Measures for Buildings of Conventional Construction.

Classification of Buildings

05402. The Classes of buildings are at para 05118.

Building Surveys

05403. When a building requires additional security measures, it is to be surveyed by professional security surveyors as detailed by PSyAs.

Key Point Surveys

05404. Establishments designated as Key Points (KPs) are to be surveyed by specialist security personnel from the Services' security organisation as detailed by PSyAs to determine the security measures required to protect them.

Points of Entry

05405. In any building housing protected material there are to be as few points of exit and entry as the functions of the site and safety considerations allow.

Securing Access Points

05406. Buildings housing protected material are to be surveyed with a view to securing all possible access points. These include the following:

a. All doors and other entrances (including inter-connecting doors with other parts of the building under separate occupancy).

b. Windows on the ground floor and other accessible windows.

c. Sunken outside areas.

d. Fuel chutes.

e. Manhole covers.

f. Parking/loading bays.

g. Electrical installations.

h. Drain pipes.

i. Roofs and openings.

Use of Security Measures

05407. Various physical security measures, such as window bars, grilles, shutters, security doors etc, can be used to protect accessible openings in the fabric of a building. Their effectiveness can be enhanced by the use of the following:

a. Intruder detection systems; see Section VII of this Chapter.

b. CCTV systems; see Section VI of this Chapter.

c. Lighting systems; see Section III of this Chapter.

d. Guard forces; see Section VIII of this Chapter.

Factors to Consider

05408. When choosing from the many security options available, the following points are to be taken into consideration:

a. **Deterrence.** The primary purpose of protective barriers is to deter intruders. They must also impose difficulty and delay on intruders who are not deterred by them, compelling the attackers to use tools, and cause noise in overcoming them. Ultimately, no practicable barrier is impenetrable given sufficient determination and the right tools.

b. **Solid barriers.** Where ventilation is not a factor a solid, rather than an 'open', barrier is preferable; a solid door will provide greater security than a grille gate.

c. **Fixed barriers.** A fixed barrier is preferable to a movable (hinged or sliding) one.

Doors

External Door Construction

05409. The following measures apply to external doors:

a. External doors are to be of solid hardwood, solid laminated core or solid multiply constructions, at least 44 mm thick.

b. Solid softwood doors ,where already fitted, can be strengthened by fitting a steel plate over the outer face of the door. The steel plate is to be of at least 18 gauge thick and is to be wrapped around the edges of the door and frame and secured on the edges and inside frame by woodscrews, countersunk and spaced not more than 100 mm apart.

c. External doors are to open outwards, because these are more difficult to force.

d. Special attention is to be paid to hinges which are to be supplemented by dog bolts.

e. Doors are to be close-fitting and equipped with suitable locks (see Section XII of this chapter).

f. Locking bars across the back of the door offer an extra layer of protection.

g. Where necessary, glass fan lights are to be barred or grilled.

h. Letter boxes are to be sealed or otherwise protected.

i. The use of an IDS can also be considered.

External Doors No Longer in Use

05410. External doors which are not used and which are not emergency exits are to be bricked up or permanently secured by screwing a steel sheet across the inside of the door frame which should be ragbolted to the fabric of the building.

External Keyholes

05411. The external keyholes of seldom used external doors are to be filled in. Padbolts (barrel bolts secured by padlocks) or heavy locking bars on the inside give further protection.

Strengthening Panelled Doors

05412. Added protection can be given to panelled doors by facing them with steel sheet, dressed round and fixed to the edges of the door.

Glazed Doors

05413. Glazed or semi-glazed doors can be strengthened by fitting a steel mesh grille to the doors. Alternatively expanding grille gates or steel roller shutters can be installed behind the doors. If it is a prestige door where unobtrusive protection is desirable, the glass can be replaced by security glazing material.

Double Doors

05414. Double doors are to be fastened by bolts attached to the first closing leaf of the door (at the top and bottom) and a security deadlock, preferably fitted with a hook-bolt attached to the other leaf. Double doors which are not final exit doors can also be fitted with internal cross bars and the second closing leaf secured with barrel bolts.

Inter-communicating Doors

05415. Doors communicating with other parts of a building under separate occupancy should in general provide a degree of security similar to that of external doors.

Internal Doors

05416. Where there is a requirement to keep doors to the basement, ground or first floor rooms locked, the keys to the locks on such doors are to be held under secure conditions but are to be readily accessible to authorised persons.

Emergency Exit Doors

Security of Exit Doors

05417. Most emergency exit locks including those of the bar release type are not fully secure and consideration is to be given where appropriate, to the fitting of intruder detection devices.

Emergency Exit Standards

05418. British standards for emergency exit devices are contained in BS 5725; those recommended for buildings holding protected assets are detailed in the Catalogue of Security Equipment held by PSyAs and other security staff.

Door frames

05419. The following applies to door frames:

a. The security of a door depends, in part, on its frame and consideration is to be given to strengthening the frame and its attachment to the surrounding building fabric.

b. Where required, doorsteps are to be reinforced by replacing wooden sills with concrete.

c. Where frames are secured by nails driven into the brickwork they can, for greater security, be fitted with steel supports to both sides of the frame and attached by steel brackets to the masonry; alternatively, expanding bolts can be used provided that they are set deep into the brickwork.

d. Where the building fabric is not suitable for bolts or steel brackets, the advice of PSyAs is to be sought regarding a satisfactory alternative.

Door Bolts

05420. The following applies to door bolts:

a. Door bolts are to be used in conjunction with security locks and fitted in pairs (at the top and bottom of the door).

b. Bolts must not be capable of being opened from outside the door and the fixing and strength of the staple are to be adequate.

c. Where the bolt engages into the floor it must engage fully and the hole in the floor is to be kept free from obstruction.

d. For securing doors on a more permanent basis padbolts with security padlocks should be used.

e. Bolts for double doors require careful selection.

f. For double rebated doors, flush bolts should be let into the edge of the first closing half of the door so that they are completely covered by the half of the door. For double doors without rebates, flush bolts with turnover levers should be fitted in the same way.

Hinges and Dog Bolts

Accessibility

05421. Hinge pins are not to be removable from outside the door neither should the hinge fixing screws be accessible from either side when the door is closed.

Reinforcement

05422. Hinges can be reinforced by fitting dog bolts near each hinge. The male half of each dog bolt is to be fitted to the hinged edge of the door and the female half to the door frame. The 2 halves interlock when the door is closed, thereby preventing the hinged edge of the door being levered away from the frame even if the hinges have been removed.

Grilles and Shutters

Use of Grilles and Shutters

05423. Expanding grille gates, roller grilles or roller shutters may be used in door-ways, passages or other openings. These may also be useful as a second layer of defence behind existing external doors, especially where there is a threat of forcible attack. Grilles may be useful in hot climates where a closed solid door is undesirable.

Frames

05424. The frames of grilles or shutters should be well secured to the surrounding structure of the building and preferably should be inaccessible from the outside of the building.

Wide Angle Optical Viewers

05425. Where it is necessary for a guard to be able to identify visitors without opening the door, or to inspect the interior of a room without entering it, wide angle optical viewers are to be fitted in preference to apertures fitted with security glass. The fitting of a convex mirror, for use in conjunction with such a viewer, may enable hidden spaces to be seen. There is to be adequate lighting to illuminate the area on the other side of the door; guards are to have access to the switch.

Windows

05426. The following security points regarding windows apply:

a. All accessible non-essential windows should be bricked up or otherwise made secure.

b. All basement, ground floor and other windows which are readily accessible are to have secure fittings.

c. Dormer windows are sometimes easily accessible from the roof of a building.

d. Window catches are to be examined and defective catches replaced.

e. Consideration is to be given to providing protection by means of intruder alarms (see Section VII of this Chapter).

f. Responsibility for securing windows at close work is to be clearly laid down in Establishment's Security Instructions.

Window Locks

05427. Some windows will require more positive protection by fitting them with window locks. The most vulnerable windows are usually those at basement or street level, those near fire escapes or verandas, or those immediately below the roof.

Use of Bars and Grilles

05428. Where it is necessary to secure a window more effectively than by the use of a lock, catch or bolt, the use of bars, grilles or shutters should be considered. The installation of intruder detection sensors should also be considered. Details of specifications for such equipment can be obtained from SSG via PSyAs.

Glazing

05429. The various types of glazing and the standards they should meet are detailed in the 'DE Specialist Construction Functional Standard - Glazing Standards for MOD Buildings subject to Terrorist Threat.' This provides an element of blast and anti-bandit protection, but not small arms or high level of intruder protection for which further advice should be sought.

Double Glazing

Advantages

05430. The following advantages accrue from double glazing:

a. Double glazing can provide excellent protection against surreptitious attack and a modicum of protection against forcible attack.

b. It is unobtrusive and can draw less attention to a sensitive area.

c. It is aesthetically more acceptable than bars and grilles.

d. Double glazing can be alarmed and has the further advantage of thermal insulation and noise reduction.

Care To Be Taken

05431. Care is to be taken with all glazing to ensure that the glazing bead or the material used to secure the glazing material to the window frame is not accessible from the outside and therefore to surreptitious attack.

Roofs

Access

05432. The following applies to roof accesses, primarily for establishments in urban areas or buildings housing sensitive information or equipment:

a. Roofs are to be surveyed to see whether there is access on to them from adjoining buildings, nearby buildings, trees, fire escapes, window cleaning equipment etc. If there is, it may be necessary to erect suitable barriers. If access is necessary, eg as part of a fire escape route, intruder alarms can be fitted.

b. Access to a building may be possible via an attic or roof space. Suitable measures to protect such means of access are to be incorporated.

c. Access from a roof into a building can in some cases be made via a chimney. If this is so, suitable measures are to be taken to block off such access by, eg, inserting a grille.

Roof Doors

05433. If the roof is accessible from neighbouring buildings or from the ground, roof access doors should be secured in the same way as other external doors.

Skylights, Fanlights, Rooflights

05434. It is possible to secure skylights, fanlights and rooflights with locks or bolts. When more protection is needed, however, one of the following is to be considered:

a. Replacing the glass with security glazing material.

b. Fitting bars or grilles.

c. Screwing the frames in place and covering the glass with steel mesh secured to the frame on the inside.

d. The Installation of intruder detection devices.

Downpipes

05435. Access to the upper floors of a building or from the roof may often be afforded by way of rainwater or soil downpipes. Such access can be restricted by boxing in the pipes or by treating them with anti-climb paint (a compound which permanently retains the consistency of thin grease). It should only be applied at heights above 2.4 m to avoid accidental contact by passers-by.

Sunken Outside Areas

05436. Buildings, not within the confines of an establishment boundary, can have sunken external areas at basement level which are accessible from the street. These can provide cover for persons seeking to gain entry through basement windows and afford convenient sites for depositing explosive or blast incendiary devices. The following is to be considered for the establishment's security:

a. The need for protection with steel grilles or steel mesh screens secured from below, providing that these do not enable easy access to the building.

b. Vents into sunken areas or vents emerging at street level are also vulnerable and may need to be fitted with internal steel grilles.

c. Access through service tunnels, fuel chutes or coal-holes can be prevented with padbolts or padlocked crossbars fitted on the inside.

d. The installation of intruder detection sensors.

Parking/Loading Bays

05437. The following is to be considered for parking or loading bays under a stand alone building in an urban area:

a. Outside working hours, they are to be closed with roller shutters or sliding shutters secured on the inside.

b. During working hours, the bays are to be under the care of a custodian or, if the threat is high, closed with electronically operated shutters which are only opened when the incoming vehicle has been identified and, if necessary, searched.

Public Utilities

Vulnerable Access Points

05438. Gas, electricity and water supply installations within buildings may offer potentially vulnerable access points, particularly in stand alone buildings in urban areas. Where possible cables and pipes are to enter the building underground. Public service meters should be so sited that access to them does not require entry

into sensitive areas. Advice on siting services entry points from the point of counter terrorist measures is given in the 'DE Specialist Construction Design Guide - Robustness Measures for Buildings of Conventional Construction.' This also gives advice on location of services within the building.

Air Conditioning and other 'Life Support' Systems

05439. Where air conditioning is essential to the operating of equipment (such as computer installations), the electricity and water supply for the air conditioning system must be given adequate protection. The measures described in Section XIII for the protection of mechanised document transfer systems are generally applicable to air conditioning systems as well. If sabotage is considered a threat, additional security measures may be required and appropriate advice is to be sought from PSyAs. Protection measures should also be assessed for other 'life support' systems such as uninterruptible power supply (UPS) and compressed air. Based on what systems are essential and under what circumstances, together with the defined threat, the works organisation and DE can determine what life support systems are then predicated. See the 'DE Specialist Construction Design Guide - Robustness Measures for Buildings of Conventional Construction'.

SECTION V TO CHAPTER 5

PRECAUTIONS AGAINST OVERLOOKING AND OVERHEARING

General

Introduction

05501. The instructions in this part relate to the threat from direct visual or photographic overlooking and non-technical overhearing only. Working accommodation and discussion areas or equipment such as VDUs or printers must be sited in order to minimise the risks of deliberate or fortuitous overlooking and overhearing.

Further Information, Advice and Guidance

05502. Information on the measures to counter the threat from electronic technical attacks such as audio-eavesdropping and the exploitation of radiation from information processing systems is detailed in Chapter 15.

Overlooking

Optical and Photographic Equipment

05503. Modern optical and photographic equipment is capable of obtaining intelligence from documents or other assets overlooked from a very oblique angle. The effective range depends on the equipment used and the prevailing atmospheric conditions but it is possible to read, or produce legible photographs of text or diagrams, at distances of 50 metres.

Precautions to be Taken

05504. Where there is a risk from overlooking the following precautions are to be taken:

a. Personnel handling protected papers or other assets are to be located out of the direct line of sight from windows or neighbouring buildings.

b. Where possible, such staffs are to be accommodated on the higher floors of multi-storey buildings.

c. Where this is not possible, the windows of overlooked rooms are to be fitted with net curtains or a translucent plastic film fixed to the glass on the inside to reduce the range from which fine detail such as typescript can be read with optical aids. It should be noted that translucent film is not effective at night if internal lights are left on.

d. Net curtains are to have a fine mesh.

e. Net curtains are to be at least double the width of the window it is required to protect.

f. Net curtains are to be hung in folds.

g. Where net curtains do not provide adequate protection because the light inside a room is brighter than that outside, opaque curtains or blinds are to be fitted.

Positioning of Vulnerable Equipment

05505. The information held-in or displayed or printed by some items of equipment can be compromised by deliberate or fortuitous overlooking. Precautions are to be taken to prevent the following:

a. Anyone overlooking the opening of a combination lock.

b. The logging-in to a password protected IT terminal.

c. The overlooking of VDUs or wall charts displaying sensitive information and printers or fax machines (siting and screening may overcome this).

Overhearing

Considering the Risk

05506. Under normal urban conditions, ordinary speech is not intelligible beyond the range of about 15 metres. In conditions of exceptional quietness or with technical aids this range may be exceeded. However, in considering the risk of over-hearing, account is to be taken of other sounds, such as traffic noise, which tend to mask speech. The risk of fortuitous overhearing is obviously increased when windows are open or when voices are raised.

Non-technical Overhearing

05507. Where there is perceived to be a real risk of non-technical overhearing, whether deliberate or fortuitous, consideration is to be given to keeping windows closed and fitting air extractors or ventilator discs to windows. At ground level, overhearing may be prevented by the erection of a fence (not necessarily a security fence) to keep potential eavesdroppers at a sufficient distance from vulnerable windows.

Ancillary Staff

05508. Care is to be taken to prevent ancillary staff, eg cleaners or contractors, from overhearing sensitive discussions.

SECTION VI TO CHAPTER 5

CLOSED CIRCUIT TELEVISION

General

Use of Closed Circuit Television for Surveillance

05601. The use of closed circuit television (CCTV) for surveillance may save manpower, especially when used in conjunction with intruder detection (IDS) and automated access control systems (AACS). It may also supplement, extend and make more effective an existing security system. CCTV enhances the effectiveness of perimeter security, particularly if used to verify the alarms signalled by a perimeter intruder detection system (PIDS).

Further Information, Advice and Guidance

05602. Further information, advice and guidance on CCTV can be obtained from the following sources:

a. Where establishments are considering the installation of a CCTV system, PSyA security staff are to be consulted to provide specialist advice and any appropriate policy input; Section II to this Chapter provides information and direction on the procurement of major security equipments and systems. In addition, where such work constitutes a works service project, the procedures detailed in Chapter 5, Section II, Annex B are to be adhered to.

b. Advice on the completion of an Operational Requirement (OR) should be sought from PSyA security staff. Additionally, further information on how to write an OR can be found in the 'CCTV Operational Requirements Manual', published by the Police Scientific Development Branch (PSDB) (Publication no 17/94). PSyA security staff should hold copies of the document.

c. DE Technical Bulletin - Uninterruptible Power Supply Requirements for CCTV Security Systems.

d. Further information may be obtained from SSG or PSDB, via PSyA security staff.

Requirement for Command Security Staff Approval

05603. Whilst the initial decision on the requirement for a CCTV system is taken at establishment level, it is essential that the quality of system ultimately procured for the establishment is of an acceptable standard and design. This is ensured by the involvement of PSyA security staffs monitoring and approving ORs from establishments to ensure that appropriate standards are maintained.

Range of CCTV Systems

05604. CCTV systems range from simple indoor or outdoor systems to complex multi-camera, low light level systems.

Type of Systems

05605. The following basic systems exist:

a. **Simple system.** In the simplest system, a camera is cabled to its own monitor, which is normally located in a manned control centre. A camera fixed to a building or some other exterior fitment provides a field of view to allow a guard to monitor, for example, control of entry into a building or secure area.

b. **Complex system.** More complex systems include cameras fitted with zoom lenses and pan and tilt facilities (normally referred to as mobile cameras), and the use of artificial lighting (either visible or infra- red) to provide 24-hour surveillance.

Applications of CCTV

05606. The possible applications of CCTV include:

a. Area monitoring; eg monitoring establishment car parks.

b. Perimeter monitoring, in conjunction with a PIDS system.

c. Pin-point monitoring, eg surveillance of equipment or entry points that could not otherwise be covered.

d. Supplementing IDS, eg verification and checking of alarms.

e. Monitoring of 'lock and leave' premises.

f. Equipment monitoring, eg video motion detectors would allow a static scene to be monitored passively and alarm only when an intrusion takes place.

System Considerations

Operational Requirement

05607. It is essential that before any purchasing action is commenced, establishments define clearly what they expect a CCTV system to do by preparing an OR. The OR is to specify the following (further guidance is to be found at Section II Annex E):

a. The areas to be monitored and the purpose for which monitoring of each area is required, eg for access control, alarm assessment etc.

b. The picture definition required in each area monitored, eg the ability to identify people and passes may be required for access control; much less detail may be acceptable for other purposes.

c. Whether linkage to an IDS is required.

d. The proposed monitoring requirements.

e. Any other performance requirements, eg meets ROTAKIN standards or ability to operate in low light.

f. Maintenance requirement/contract arrangements.

g. System security measures such as anti-tampering, lightning protection or un-interruptible power supply.

ORs are to be agreed by PSyA security staff before being used as the basis for any system procurement.

Site Survey

05608. A site survey is to be carried-out under the auspices of the PSyA security staff utilising professional security staff (e.g. SSG staff – Annex A refers) by day and by night (if night surveillance is required) and is to include the following points:

a. **Terrain.** Differing backgrounds give widely differing results from the same camera, eg asphalt, open grassland, hangars, red brick buildings, etc.

b. **Climate and environment.** Heat, ice, high rainfall, condensation, dust, etc can adversely affect camera performance. Cameras may be blinded by snow, fog, heavy rain or smoke. Special features, eg sun shades, wipers, heaters may be required;

c. **Existing light sources.** Existing light sources must be identified; those which may impair camera performance must be screened or cameras sited to avoid them; these may include street lights, security lights, sunrise, sunset, reflection of sun from water, windows, etc.

Camera Trials

05609. Following, or as part of the site survey, recorded camera trials are to be carried out to ensure that proposed camera positions and equipment (fences, lighting etc) meet the OR in appropriate lighting and weather conditions. ESyOs are to maintain a Record of View for each installed camera so that following maintenance/replacement, the same field of view is achieved. The ROTAKIN is to be used in such trials.

Audit of System

05610. An audit of the CCTV system is to be carried out by professional security staff.

Uninterruptible Power Supply

05611. Where there is a requirement for a CCTV system to have an un-interruptible power supply, the provisions of the 'DOE Technical Bulletin – Un-interruptible Power Supply Requirements for Closed Circuit Television Security Systems' may apply. The document is advisory only and is held and used by Property Managers, Defence Land Agents, Establishment Works Consultants, Works Service Managers, Project Staff Officers, Project Sponsors and Project Managers. Television security systems associated with cameras operating in critical security positions should have a facility that enables it to continue operating under all mains failure conditions. Television cameras in less critical security positions will need to have their power supply requirements assessed on an individual basis.

The ROTAKIN

05612. The ROTAKIN is a test target, which has been designed by PSDB to simplify the job of establishing and maintaining an effective CCTV system. It is essentially a silhouette of a person 1.6m high. On it are high contrast patterns. It is used to:

a. Ensure complete coverage of the area required.

b. Assess the system coverage and image size.

c. Perform repeatable tests of picture quality.

System Security Policies and Security Operating Procedures

05613. Where CCTV is computer-controlled, appropriate system security policies (SSPs) and security-operating procedures (SyOPs) must be issued for the system.

Video and Disc Recording

5614. Time lapse video tape recording enables pictures covering periods of up to 300 hours to be recorded on a single reel. The ability to record and play back is a useful feature for recording and investigating alarms. Loop framestores are available using discs which continually over-write onto a disc; when a alarm is triggered, it commences recording frame by frame including retrieving pictures a specific time before the alarm activated. Loop framestores are especially useful if control room operators have duties that can stop them responding immediately to alarms. For loop framestores to be useful, alarm and CCTV systems have to be working well. If the false alarm rate is high, or if CCTV coverage is incomplete, then a loop framestore will not help.

Video Movement Detection Systems

General

05615. Video movement detection (VMD) equipment monitors the video signal for movement or changes in light intensity in the picture and provides an alarm to the reaction force (normally an audible signal to alert the guard coupled with a visual indication on the monitor). The sensitivity of the equipment to motion or light changes needs to be adjusted for site conditions.

Range of Systems

05616. Systems range from a single camera processor and monitor system to groups of cameras whose video signals are constantly assessed by a single processor. Devices are available which can cope with the widely varying light conditions encountered in the open; many are technically limited and suitable for interior use only.

Limitations

05617. Video movement detectors have considerable limitations in practice. Video movement detector cameras, although providing reasonable cover for external scenes, may be blind in adverse weather conditions, and are ineffective where there is a high level of legitimate movement. However, it is possible with some systems to block out areas where movement occurs.

This page left intentionally blank.

SECTION VII TO CHAPTER 5

INTRUDER DETECTION SYSTEMS

General

Aim of Intruder Detection Systems

05701. Intruder detection systems (IDS) are designed to detect the entry, or attempted entry of an intruder into a protected area, to identify the location of the intrusion and to signal an alarm to a reaction force. Correctly installed, performance tested and employed IDS can result in savings in security manpower. To be effective, an IDS must have a response force that will react in the event of an alarm condition.

Further Information, Advice and Guidance

05702. Further information, advice and guidance on IDS can be obtained from the following sources:

a. Where establishments are considering the installation of an IDS system, PSyA security staff are to be consulted to provide specialist advice and any appropriate policy input; Section II to this chapter provides information and direction on the procurement of major security equipments and systems. In addition, where such work constitutes a works service project, the procedures detailed in Chapter 5, Section II, Annex B are to be adhered to.

b. Advice on the completion of an Operational Requirement (OR) should be sought from specialist security staffs.

c. Further information may be obtained from Special Services Group (SSG), via PSyA security staff.

d. The use of an IDS to support or as an alternative to guards, is covered in the minimum baseline measures for physical security (see Section I).

Requirement for Command Security Staff Approval

05703. Whilst the initial decision on the requirement for an IDS is taken at establishment-level, it is essential that the quality of system ultimately procured for the establishment is of an acceptable standard and design. This is ensured by the involvement of PSyA security staffs monitoring and approving ORs from establishments to ensure that appropriate security equipment standards are maintained.

Intruder Detection Systems

5704. IDS systems have been graded according to the level of security they offer with a Class 4 system offering the highest level of security and a Class 1 the lowest.

a. **Class 4 systems.** An alarm system for use in applications where security takes precedence over all other factors. It is intended to give a level of protection where the intruder is expected to plan the intrusion in detail and have a full range of equipment capable of substitution of vital system components. A Class 4 system requires to be supplemented with comprehensive physical security measures and security procedures.

b. **Class 3 systems.** An alarm system used in establishments where high value assets are held. Such a system is to include appropriate physical security protection. The system is to offer protection from intruders who are conversant with IDS and have available a comprehensive range of tools and portable electronic equipment.

c. **Class 2 system.** An alarm system where the risks of sophisticated attack are not high. Intruders are expected to have a limited knowledge of alarm systems and have available only basic tools and portable instruments.

d. **Class 1 system.** An alarm for use in low risk establishments where potential intruders have little knowledge of alarm systems and a limited range of readily available tools.

The SEAP approved IDS panels are at Section I, Annex E.

Uses of IDS

05705. The following factors concerning IDS are to be considered:

a. An IDS provides continuous surveillance over the protected area and may help to reduce guarding requirements.

b. In certain circumstances it can substitute for guards or alternatively, when used in conjunction with guards, may extend coverage into areas not normally accessible to guard patrols eg roof space or locked rooms.

c. It is to be fully integrated into the other security measures on an establishment in order to apply the principal of 'Defence in Depth'.

Operational Requirement

Compilation

05706. IDS are expensive and care is to be taken in the selection, application and installation of an IDS to prevent it being circumvented or its usefulness being impaired by a high incidence of technical problems or false alarms. An Operational Requirement (OR) is to be compiled by the establishment after consultation with and approval by PSyA security staff. Establishments are to define clearly what they expect of an IDS and to be aware of its limitations. In setting the requirements for an IDS installation the following is to be specified:

a. The area/equipment to be protected.

b. The detection performance required and how it should be tested.

c. Acceptable false alarm rate.

d. Any special requirements affecting the areas concerned and the degree of security protection necessary.

e. Whether linkage to other electronic systems such as CCTV or AACS is required.

f. The overall security plan and details of all related measures relevant to the design of the system.

g. The type of reaction force or monitoring arrangements required.

h. The position of the alarm display panel and details of related security procedures.

Further guidance on the production of the OR is to be found at Section II, Annex E.

Site Survey

05707. Following approval of the OR, a site survey is to be arranged by PSyA security staff (who may task their single-Service security organisation, or SSG). The site survey is to consider:

a. The type of asset requiring coverage.

b. The perimeter length requiring coverage.

c. Whether there is sufficient ground available to establish sterile detection zones on the attack side of each area.

d. Type of building, where appropriate, that the IDS is to be provided for.

e. Prevailing weather, topography and local wild life.

f. The resources, including CCTV and guards, available for alarm verification.

See also Section II for co-ordination of security aspects of works services.

Audit of System

05708. An audit of the IDS system is to be carried out by professional security staff.

System Components

05709. An IDS installation is to include some or all of the following system components:

a. Detection sensors.

b. A control panel with optional event recorder and printer.

c. An alarm display.

d. Installation wiring.

e. An alarm signalling link between the control panel and alarm display.

f. A reaction force.

g. An independent, uninterrupted power supply as appropriate.

Detection Sensors

05710. Detection sensors are designed to detect an intrusion within the area they cover and to provide an indication to the control panel of the alarm condition. Various types of sensors can be used in combination, particular at high-risk sites, to cover technical vulnerability, reduce the incidence of false arms, and provide against failure. IDS sensors are to be fitted on the points of entry, i.e. doors and windows. Further coverage inside rooms and of security containers provides a second-line of defence.

Types of Sensor

05711. The types of detection devices available are divided into the following categories:

a. **Contact sensors.** Contact sensors cover various switching devices such as micro-switches, magnetic reed switches, pressure pads and some types of vibration sensors.

b. **Spatial or volumetric sensors.** Spatial or volumetric sensors are designed to detect movement within their field of view and are used to cover rooms, corridors, roof spaces and other open areas or entry routes.

c. **Ultrasonic sensors.** Ultrasonic sensors use high frequency sound waves and the Doppler effect of radiated and reflected transmissions.

d. **Passive infra red sensors.** Passive infra red sensors (PIR) monitor the infrared heat profile of an area and detect changes caused by human intrusion.

e. **Microwave sensors.** Microwave sensors use high frequency radio transmissions and reflection to detect movement.

f. **Beam interruption devices.** Beam interruption devices are usually of the active infra-red type which use a transmitter and receiver and sometimes reflecting devices to project a beam across an opening such as a door or window. When the beam is broken either by the opening door or window or by a person passing through it an alarm is raised.

g. **Vibrations.** Vibrations can be detected by various devices or technologies. The Inertia switch reacts to vibration or impact by a contact ball bouncing or lifting off its contacts and producing an alarm condition; a Geophone detects movement by a suspended magnet moving inside a detector coil; and the properties of Piezoelectric Crystal in producing an electric current from structural pressures can be used to detect vibrations and raise an alarm.

h. **Dual technology sensors.** Dual technology sensors are devices that combine two sensor technologies (PIR and microwaves) in one housing and where they work together before signalling an alarm. In this way the likelihood of false alarms is greatly reduced.

Control Panel

05712. The main functions of a control panel are to:

a. Monitor the state of the detection sensor(s).

b. Detect tampering.

c. Provide the means for setting and un-setting the system.

d. Signal an alarm state.

Event Log

Electronic Log

05713. Control panels built around a microprocessor are to include an electronic log or event recorder that can be linked to a hard copy printer. The log is to provide a record of all alarms and operational instructions, such as "setting" and "un-setting" of the system. It will also provide an aid to monitoring the security of the system and providing an audit trail.

Location of Event Log

05714. Unless the control panel is situated at a permanently manned guard point, it is to be located at the heart of the IDS installation where it is given maximum protection by the system itself and by other physical security measures.

Alarm Display

Alarm Signalling

05715. Currently, alarms may be signalled in the following manner:

a. **Audible/visible.** Flashing beacons and/or gas powered hooters on buildings eg a Patrol Warning System as used on aircraft storage or explosive storage buildings within a secure perimeter. However, this type of alarm should not be considered for new builds or as part of refurbishment programmes.

b. **Remote sites.** An alarm may be signalled to a permanently manned control position and may indicate a loss of power, tamper or open door. These alarms allow a controlled response force reaction.

Alarm Signalling for Remote Sites

05716. Some form of remote alarm communication signalling to an alarm monitoring station is to be provided where the protected site is not permanently guarded. Alarm signalling can be by means of:

a. **Hard wired/fibre optic cabling.** Where there are existing hard wired/fibre optic cabling, the viability of using them or their cableways should be examined.

b. **Private lines.** Private lines are direct telephone lines used exclusively for alarm signalling and monitoring. This system provides protection against 'shorting out' or cutting the lines, which will cause an immediate alarm.

c. **Auto dialling.** Auto-dialling uses a standard exchange telephone line and equipment that, when an alarm is raised, automatically dials an emergency call number and relays a pre-recorded message.

d. **Radio links.** Radio-links provide a multi-path communications system, which can incorporate a number of features such as automatic paging, data encryption and two-way, interrogation and response, protocol.

Installation Wiring

05717. The installation wiring in a high security system is to be monitored, automatically, at all times, i.e. there should be continuous electronic examination of the circuit connections to ensure that they are in working order and are not being tampered with. There should be an immediate alarm if a fault occurs or line tampering is detected.

Reaction Force and Response Time

05718. Provision is to be made by the establishment for a reaction force drawn from an approved guard force (eg establishment guards) or in certain circumstances, with TLB staff approval, local police forces may provide a response force.

System Management

05719. The IDS system manager is to have TORs issued by the HOE.

System Security Policies and Security Operating Procedures

05720. Where IDS or PIDS are computer-controlled, appropriate system security policies (SSPs) and security-operating procedures (SyOPs) must be issued for the system.

Installation and Maintenance

Secure Installation and Maintenance

05721. The security of an IDS depends on secure installation and maintenance. To ensure any system continues to provide its optimum performance, performance testing, servicing and preventative maintenance is needed. These tasks should keep costs down and maintain acceptable performance. To ensure that appropriate safeguards in relation to installation and maintenance, are put in place, establishment security staff are to ensure that the following is actioned:

a. Circuit diagrams, manuals and spares for IDS installations are to be kept under secure conditions.

b. All installation and maintenance work is to be carried out by authorized personnel and supervised by establishment security staff.

c. Any modifications to the system are to be agreed by the system manager and Security Authority. A record of the modification is to be held with the original specification or diagrams.

d. Class 4 systems are to receive at least 4 maintenance visits per year and Class 1 to 3 systems are to receive a minimum of 2 visits. The high maintenance requirements for Class 4 reflects that the system is protecting

high value/ sensitive assets and the Head of Establishment must have confidence in the system's integrity and be aware of the need to maximise the system's availability.

e. Defence Estates has negotiated a Supply Services Agreement with SSG for the maintenance of Class 4, AC12 based, alarm systems. AC12 systems, if not maintained by SSG, will not be allowed to maintain Class 4 status.

Standby Power

05722. The following measures apply to standby power:

a. A standby power supply is to be available to enable the IDS to continue operating in the event of the main power supply failing or being disconnected.

b. Float charge batteries can be used for standby power. They should have a sufficient capacity to cope with foreseeable contingencies.

c. The condition of batteries is to be regularly checked by authorized personnel.

Alternatively, the installation of an un-interruptible power supply (UPS) can be investigated.

05723. *Spare.*

Access Control Panel

Access

05724. The following applies:

a. An IDS is only to be "set" or "unset" by authorized personnel.

b. The control panel is to be positioned and protected such as to deny access to all but nominated personnel.

c. Where a control panel is key operated the key is to be treated as a security key and afforded the appropriate protection.

d. Operating codes are to be protected in the same way as combination lock settings or system passwords.

e. Where the control panel is sited within an area that is not permanently supervised it is to be secured in an approved security container. The container is to be kept locked and protected by the IDS.

f. Unauthorised personnel are not to have access to installed IDS sensors.

g. The tamper alarms are to be monitored 24 hours and the correct operation of all sensors is to be checked at regular intervals.

Testing

05725. The testing of IDS is to be by the activation of a sensor to check that an alarm has been raised. IDS installed in high security sites are to be tested at least once a day.

Where this is not possible, they are to be tested regularly at intervals to be prescribed in establishment security regulations and reporting action for malfunctions specified accordingly. For testing of IDS on armouries and ammunition stores, see Chapter 6.

Event logs

05726. Where event recorders are fitted the following applies:

a. The log is to be examined regularly by establishment security staff and compared where appropriate with reports submitted by the guard force.

b. Personnel are to be trained to recognise the development of a suspicious sequence of events and have the authority to investigate incidents such as mains failure.

c. Where a hard copy print out of events is obtained, it is to be stored for a period of 3 years to allow for retrospect analysis and investigations.

Investigation of Alarms

05727. In the event of an attack being mounted on an IDS, a sensor may give only one warning before it is circumvented. Therefore each alarm is to be thoroughly investigated by the establishment security staff and every attempt made to establish the cause. Personnel are to be made aware that a sequence of unexplained alarms occurring over a prolonged period of time can indicate that probing attacks are being carried out or that an attacker is attempting to undermine confidence in the system.

Refurbishment of Buildings

05728. When a building or individual suite of offices is refurbished after an IDS has been installed, the rearrangement of partition walls and the re-positioning of security

containers or protected equipment can reduce the level of protection originally provided by the IDS. ESyOs are to ensure the following:

a. Where necessary a survey is carried out, and the IDS installation adapted to the new accommodation arrangements.

b. Building works are to be prevented from having unsupervised access to components of the IDS, and a thorough check of the system is to be carried out once the work is completed.

c. Where major alterations are involved, consideration is to be given to the de-commissioning of the IDS altogether.

Portable Intruder Detection Systems

05729. Portable or transportable IDS can be a cost effective method of providing security for large items of equipment in the open such as aircraft, ships in dock or armoured vehicles and can be used inside buildings to protect equipment or provide an extra layer of security on an establishment. They also have the advantage that they can be deployed on Out-Of-Area (OOA) operations to assist the detachment guard force

ANNEX A TO SECTION VII

THE AC12 INTRUDER DETECTION SYSTEM

Defence Estates (DE) and SSG have an agreement regarding the installation and maintenance of the AC12 IDS and all questions on these topics should be referred to DE through establishment property managers.

This page intentionally left blank.

SECTION VIII - GUARDS AND PATROLS

General

05801. These instructions are for use only at non-nuclear sites. Separate instructions for the protection of nuclear sites are contained in JSP 440, Volume 4. The following instructions are mandatory, unless otherwise stated in the text, and any measures relating to the arming of guards, patrols or QRFs (including those provided by the MDP) may not be the subject of waivers or exemptions without the written authority of the TLB. If TLBs elect to delegate this authority it is not to go below 2-star level (Divisional/District Comd or equivalent). Under these circumstances, the TLB is to be informed on each occasion that a decision to grant a waiver/exemption is taken. The TLB is then to inform DGS&S. Notification is to be accompanied by the rationale for the decision. This is to include an explanation on what measures have been taken to minimise the risk. Procedures to be followed by HOE seeking waivers/exemptions and for TLB Principal Security Advisors (PSyA) staffs when processing such applications, are contained in JSP 440 Volume 1, Chapter 2, Section 5.

05802. Further information, advice and guidance on guards and patrols can be obtained as follows:

a. Further guidance on the use of patrols and guarding in the Counter Terrorist context can be found in JSP 440, Volume 1, Chapter 7.

b. MOD Instructions for the Use of Commercial Guard Forces in Great Britain are contained in JSP 440, Volume 1, Chapter 18.

c. Guidance on the arming of guards can be found in The Carriage of Arms Directive to CINCs - DCDS(C)/06/04/01 dated 19 Nov 98 and JSP 440, Volume 1, Chapter 7.

d. Guidance on the Issue and Use of Batons by Service personnel can be found in JSP 440, Volume 1, Chapter 7, and in Card E of JSP 398, the compendium of UK National ROE.

e. Advice on the preparation of Guards' Orders can be obtained from the TLB Principal Security Advisers (PSyAs).

f. The use of guards within the minimum baseline security measures is covered in JSP 440, Volume 1, Chapter 5, Section 1.

g. Card B of JSP 398 gives guidance for Service personnel dealing with trespassers on MOD property.

h. Card A of JSP 398 gives guidance for opening fire for Service personnel authorised to carry arms and ammunition on duty in the UK.

Definitions

05803. The following definitions apply throughout this chapter:

a. **Armed Guard.** An armed guard is a guard, armed with an official issue firearm, on duty. Only Service personnel and the MDP are permitted to carry firearms.

b. **Guard with baton**. A guard equipped with a defensive weapon such as a Baton (Paragraph 05802 d. refers). Only single-service/CCMDP approved batons are to be issued for the purpose of self-defence.

c. **Unarmed Guard**. An unarmed guard is a guard on duty at a specific point, not equipped with a firearm or baton.

d. **Quick Response Force (QRF)**. A QRF is a formed body whose duty is to respond to any security incident at any establishment within their area of responsibility. Their duties and responsibilities are to be clearly defined in their orders. Clear instructions must be given regarding Command and Control aspects, which must have been agreed in writing between the HOE and the person in charge of each element of a combined service QRF if they are not under command of the HOE. The QRF, which may be located either on or off site, must be capable of responding to an incident in time to be effective. If armed guards are on duty at the establishment, the QRF must also be armed, and must, therefore, be found from either Service police or personnel, MDP or a Civil Police Force (CPF). The size and geography of the site being protected will determine the size of the QRF but if armed, it must comprise at least two people. QRFs are not to comprise a mix of armed and unarmed personnel. The objectives of an armed QRF are:

(1). To provide an immediate armed response to incidents where life is threatened.

(2). To provide initial containment at such an incident pending the arrival of support unless exceptional circumstances necessitate immediate action (within the limits of the Rules of Engagement) to save life or prevent harm or injury to any person.

e. **Patrols**. Definitions of patrols and their frequency in the context of the Minimum Baseline Measures Matrix (MBMM) are at Section I, paragraph 05122. Further definitions of Point Guards and Dog Patrols in the context of the security of equipment MBMM are at Section 18.

Principles of Guarding and Patrolling

Guard Forces

05804. Guards within the MOD are drawn from the following sources:

a. Service police.

b. Service personnel.

c. Ministry of Defence Police (MDP).

d. Ministry of Defence Guard Service (MGS).

e. Commercial Guard Forces (CGF).

Security Duties

05805. The main security duties of a guard force are as follows:

a. To deter unauthorised intrusion to the site being protected.

b. If deterrence fails, to detect intrusion as early as possible and to detain the intruders until the arrival of the police or other support.

c. To react to any security incident which may occur.

d. To conduct the following specific tasks:

(1) Access control.

(2) Supervise the arrival and departure of vehicles.

(3) Undertake patrols.

(4) Monitor intruder detection systems (IDS), site access management systems (SAMS) and automatic access control systems (AACS), including closed circuit television (CCTV).

(5) Control and issue keys.

(6) Establish a security control centre for the establishment.

(7) Inspect and check perimeters, security communications, IDS and perimeter lighting.

(8) If appropriate, provide a nominated QRF, armed if armed guarding has been ordered.

Arming Policy

05806. Arming policy is currently laid down in CDS 21/90. The related Arming Directive is at DCDS(C)/06/04/01 dated 19 Nov 98 and JSP 440, Volume 1, Chapter 7.

Weapons

05807. Only SA80 (IW/LSW) or 9mm SLP with standard ball ammunition may be issued to Service personnel or MDP on general security duties, unless written authority from CINCs (or delegated 2-star authority) or CCMDP is held for the use of other weapons. When weapons with an automatic fire capability are issued, only the single shot mode is to be used. Weapons must be correctly zeroed.

05808. Before Service personnel or MDP are issued with arms and ammunition for employment on general security duties they must receive adequate training in weapons handling, safety, marksmanship and the Rules of Engagement as laid down by CINCs, and CCMDP.

05809-05810. Spare.

Categories of Defence Establishments for Guarding Purposes and Composition of Guard Force

05811. Defence Establishments are categorised for guarding purposes; the category will determine the mandatory minimum guarding requirement for that establishment. This categorisation does not include Cadet Units, to whom Chapter 6 of Volume 1 refers, or nuclear establishments, the security policy for which is covered by JSP 440, Volume 4. In order to avoid confusion with the categorisation used in JSP 440 Volume 1, Chapter 2, Section 2 for general security purposes, the numbers are preceded by the letter P (for Priority)[1]:

a. **P1**. Buildings and areas (excluding Service Families Accommodation (SFA) areas) in which identifiable and/or uniformed Service personnel live overnight on a regular basis, or are permanently occupied for work (examples are barracks, communication sites manned over 24 hours). These establishments must, at all times, be protected by a guard force capable of being armed. If armed guarding has been ordered, an armed guard is to be posted at each active entrance/exit (for more detail on Control of Entry see JSP 440, Volume 1, Chapter 5, Section 9) and an armed Quick Response Force (QRF) must be permanently available. Armed personnel guarding

[1] Armed Forces Careers Information Offices are not included in this categorisation. Separate instructions are contained in Chapter 7, Paragraphs 07069 to 07076 and Annex M.

gates may be included in the QRF provided their gates can be closed and secured for the duration of the alert. At least one gate will need to remain in operation for possible access of emergency services.

b. **P2**. The following buildings and areas:

(1) Those in which identifiable and/or uniformed Service personnel work on a regular basis, e.g. normal working hours on weekdays (frequently in conjunction with MOD civilian employees).

(2) Those where weapons, ammunition and explosives considered to be Attractive to Criminals and Terrorist Organisations (ACTO)[2] are stored.

These establishments must at all times be covered by a QRF capable of being armed. QRFs found from MOD sources must be armed if armed guarding has been ordered. If the QRF is found from a CPF, decisions on arming will rest with the police chain of command. Permanent static armed guards at entrance/exits are not required.

c. **P3**. Other buildings and areas:

(1) Those in which people live and work on a part-time, irregular basis, e.g. certain training camps.[3]

(2) SFA areas and buildings and areas, outside the scope of P1 and P2, which are recognised MOD/Service social centres, e.g. NAAFI Clubs, Recreation Clubs or Messes in which people are not accommodated.

(3) Wholly or predominantly civilian manned Defence establishments. This will include the majority of retained DERA (DSTL) and DPA sites. Service personnel employed at these sites should wear civilian clothing, unless their function demands that uniform be worn (in line with the guidance on the wearing of uniform in public, contained in JSP 440, Volume 1, Chapter 7 and local orders/instructions). Security advisory staff will then advise whether the establishment should be categorised as P2.

---

[2] For definition of ACTO see Chapter 6, Section I, Paragraph 06004b.

[3] Some training camps are used so extensively that they need to be treated as if they were regularly occupied.

Armed guards and QRFs will not normally be deployed at these establishments except at BIKINI alert states AMBER or RED. Heads of Establishments (HOE) are to make appropriate contingency plans for periods of increased alert state.

Duties of Guards

05812. The specific duties of guards vary with circumstances but will include the following:

a. **During working hours.**

(1) Control entry.

(2) Supervision of maintenance staff working in places where protectively marked material is kept.

(3) Dealing with and reporting any security incidents to the establishment's security advisers.

(4) Monitoring any CCTV, AACS, SAMS and IDS and responding to alarms.

(5) Carrying out mobile, foot and dog patrols where appropriate.

b. **At cease work.**

(1) Ensuring that all windows, doors, skylights, gates, etc are secure.

(2) Checking that all security containers are properly locked and that no protectively marked material (including waste) has been left out.

(3) Carrying out mobile, foot and dog patrols where appropriate.

c. **Outside working hours.**

(1) Carrying out mobile, foot and dog patrols where appropriate.

(2) Supervising cleaners, maintenance and other ancillary staff in the building or area (where so detailed).

(3) Monitoring any CCTV, AACS and IDS; responding to alarms.

(4) Dealing with visitors and deliveries.

Control of Entry

05813. All in-use entrances/exits to/from establishments are to be guarded by at least one person. In P1 establishments, if armed guarding has been ordered, at least one of these guards is to be armed. Where circumstances permit, an armed guard may undertake control of entry duties on his own. At busy entrances with a number of vehicle checkers an armed cover guard is to be posted (and this guard may constitute the sole armed presence). Internal control of entry to sensitive buildings/areas need not include an armed element unless local circumstances or other MOD directives require otherwise. If an Automatic Access Control System is in use, the HOE is to decide whether a guard is required or not (with advice from the PSyA). The decision will depend upon the prevailing alert state and local threat assessment.

Internal Patrols

05814. Internal patrols are to be mounted to cover those areas that are considered likely terrorist targets (e.g. barracks accommodation, messes etc) which are not covered by electronic surveillance systems or static point guards. In category P1 establishments, patrols should have an armed element if armed guarding has been ordered. In daylight hours, patrols may consist of one person, but during the hours of darkness the need for 2 man patrols should be considered. Emphasis should ideally be placed on foot patrolling during the hours of darkness. The number and frequency of these patrols is to be decided by the HOE.

External Patrols

05815. Off-base patrolling by armed Service personnel or MDP may only be undertaken with the express written agreement of the Chief Constable of the local CPF[4], who is responsible for the policing and security outside the perimeter of a Defence establishment.

Search

05816. Powers of search. HOE are to issue clear concise orders on Powers of Search in their Establishment's Orders for the Guard. Guard Commanders are to ensure that their subordinates are aware of their orders. The MOD policy for searching is at Annex C to this Chapter.

05817. Spare.

[4] External patrols by MDP officers are authorised by the Consolidated Policing Protocol which is an agreement between CCMDP and the Association of Chief Police Officers (ACPO) for England and Wales and ACPOS in Scotland.

Trespassers

05818. Specific guidance for Defence personnel on dealing with trespass on MOD property is at Card B of JSP 398. This guidance was developed primarily to deal with demonstrators but the direction it contains can equally be applied to dealing with suspected terrorists or other intruders. HOE are to ensure that all personnel employed on security duties are familiar with the requirements of Card B. COs/HOE are to ensure their personnel understand their powers of arrest and, where applicable, the local bylaws and Acts of Parliament which give additional powers of arrest to Defence personnel.

Response Plan

05819. Each unit/establishment is to have a response plan. There must be a nominated QRF (see Paragraph 05803d above) which, in Category P1 and P2 establishments must be capable of being armed and be armed, if armed guarding has been ordered. The QRF can be found from a unit/establishment's own resources, a neighbouring establishment, the MDP or local CPF. The QRF must be capable of mounting a swift[5], effective response to either a terrorist attack, a request for assistance from a member of the guard force or to an Intruder Detection Alarm activation. The duties and responsibilities of the QRF must be clearly stated in their orders. It should be noted that the initial response by a CPF might well be provided by unarmed police officers.

Static Posts

05820. In addition to the static posts at the control of entry points, further static guard posts may be established at the discretion of the HOE. In Category P1 establishments, these posts should have an armed component if armed guarding has been ordered.

Cadet Units

05821. Members of Cadet Forces are authorised to carry out the following security duties:

a. Officers and Adult Instructors (AI) may carry out general security duties, including protection of arms and ammunition stores, but they may not be armed with firearms. They may be equipped with batons for self-defence, provided they have received adequate training in their use in accordance with policy on the use of batons. Except at camps, they should only carry out

[5] As a guide, a 'swift, effective response' will not normally exceed 10 minutes to mount.

security supervisor duties, in addition to any necessary action to search and secure premises on initial occupation or to check vehicles before use.

b. At cadet camps, cadet officers and AIs must expect to carry out duties which may include the duties of sentry/prowler guard in accordance with Cadet Force regulations.

c. Cadets may carry out guard duties during daylight hours only (and normally not later than 2200hrs) in accordance with Cadet Force regulations. They may not be armed and must not be issued with batons, pick-helves or any other type of weapon. Cadets are not to guard armouries or ammunition stores.

Use of Regular Defence Training Camps Alone

05822. Whenever Cadet units use Regular Defence Training Camps alone the guarding requirement will cause a dilemma. The officer in charge is to draw up security standing orders based on the same general counter measures as those in force with Regular and Reserve Forces units. There is no requirement to provide armed guards for the protection of cadet force personnel. Their presence as cadets is to be well advertised. It is possible that Cadet Force units' own resources will be insufficient to give the required degree of protection. In such circumstances they are to be supplemented as necessary under arrangements made by the appropriate formation headquarters. The following supplementary resources should be considered:

a. Regular Service personnel who may, in any case, be provided to assist with cadet training. Where they are not already being provided, their provision specifically for guarding should be considered. Wherever regular personnel are provided for guard duties, they are to be armed for their own protection, if armed guarding has been ordered.

b. Contract security personnel may be used to supplement other categories of guard so long as they are under command of military or adult Cadet Force personnel.

c. MDP (armed if appropriate). In particular the use of Area Policing Teams is advised. The APT should be requested to make frequent, irregular visits to the establishment and its surrounds.

d. MGS.

Guard Funding

05823. There are no funds specifically allocated for contract guards or temporary civilian patrolmen for Cadet Force security. Where regular Service personnel, MDP

or established recognised guard forces cannot be made available, the appropriate formation headquarters will decide whether cadet training is to proceed or not.

Use of Ranges and Training Areas

05824. When using ranges and training areas, Cadet Force units are to follow the following guidelines:

a. Entry points such as gates, firing points, target galleries, huts and tents etc are to be thoroughly checked on arrival by an AI, secured throughout the period they are in use, and checked again by an AI immediately before departure.

b. Transport is to be parked in a secure area or guarded.

c. On departure, the doors and window shutters (if fitted) are to be locked and the keys returned to the relevant authority.

05825. Spare

Accommodation and Equipment

Guard Force Efficiency

05826. To ensure the efficiency of the establishment guard force, the following applies:

a. Adequate, properly equipped and scaled accommodation is to be provided in accordance with JSP 315.

b. Accommodation is to include an incident control room and suitable accommodation and rest areas.

c. Guards are to be suitably equipped with vehicles, communications equipment, torches, etc.

d. The force size is to be adequate to cover detachment, leave, courses and sickness.

Access to Protectively Marked Material by Guard Forces

05827. The following principles apply to access to protectively marked material by the guard force:

a. Guards will not normally have access to protectively marked material or to keys giving access to such material.

b. Normally they will not enter secure rooms or strong rooms unless supervised by someone with authorised access. Nevertheless they are to check the doors of such rooms (and any other locked rooms) during their normal patrols.

c. Guards are to be permitted access to restricted areas out of work hours to check for possible security breaches. Where this is not possible, arrangements are to be made to cover the restricted area by the use of alarm sensors or CCTV surveillance.

Security Clearance for Defence personnel

05828. Defence personnel guarding protectively marked material or patrolling inside security areas are to be appropriately cleared for the highest protective marking to which they might inadvertently have access. The rules for commercial guard forces are described below.

Commercial Guard Forces

Commercial Guard Forces in GB

05829. Commercial guard forces (CGF) may be employed by the MOD in GB. JSP 440 Volume 1, Chapter 18 contains mandatory security instructions for MOD authorities directly or indirectly concerned with the employment of CGF. All members of CGF employed by the MOD are to have a Basic Check (BC) and Counter Terrorist Check (CTC) carried out on them. All unarmed guarding tasks may be undertaken by CGF (see JSP 440 Volume 1, Chapter 18, Paragraph 1807). The use of CGF in Category A establishments must be carefully considered, with due regard being paid to the tasks the CGF will be required to undertake and the appropriate levels of security clearance required.

Other Considerations

05830. Transition to war (TTW)/war role, or likely changes in the future use of the site, may render it unwise to employ CGF on some tasks irrespective of the level of protection provided for physical security purposes. The PSyA should also seek advice on the likely impact of European legislation on employment conditions, e.g. TUPE, and the Working Time Regulations (and its associated entitlements) in force in GB. Such considerations may have an impact on the decision to employ CGF at all, and could introduce long term financial penalties.

Commercial Guard Forces Outside GB

05831. Whilst the MOD security instructions referred to in para 05829 are mandatory in GB, they may also be useful as guide lines for MOD authorities outside GB when considering the employment of CGF. In such circumstances, the appropriate PSyA is to be consulted at the outset.

05832 - 05835. Spare.

Supervision of Guards

05836. Supervisors are to make unannounced daytime/out of hours visits to ensure that guards are undertaking their duties correctly, understand their orders and have, if necessary, submitted written reports in respect of incidents. Supervisors should initial the Daily Occurrence Book (DOB) and personal notebooks (if issued) during visits to guards.

Instructions

Written Orders

05837. Mandatory instructions, in the form of written orders and SOPs are to be provided to Guards and QRFs and are to:

a. Be clear and concise, and up to date.

b. State the buildings, rooms and security containers to be inspected by patrols.

c. Provide the details of names, addresses, and telephone numbers of personnel to be informed of incidents.

d. Where appropriate, give orders on how to secure buildings out of hours including a list of doors, windows, fire escapes, skylights etc. that need to be checked.

e. State the frequency of patrols.

f. Detail the action to be taken:

(1) Whenever a breach of security is discovered.

(2) When mail is received out of hours.

(3) Whenever an intruder is discovered.

(4) When a fire, bomb alert, hoax call or other emergency occurs.

(5) When calling out reaction forces.

g. Detail the use of firearms, including ROE, including the responsibility for the issue of arms and ammunition to the guard force.

h. Detail the maintenance records and production of security reports.

i. Detail the safekeeping of keys.

j. Detail the supervision of maintenance and other ancillary staff.

The orders are to be reviewed on a frequent basis and are to be available for inspection by the PSyA.

Signing of Orders

05838. A record sheet is to be maintained on which each guard signs as having read and understood the orders. Guards are to sign such a record in the following circumstances:

a. Prior to a 'set' of duties, in the case of Service personnel employed occasionally on guard duties.

b. Every 6 months (or more frequently at the direction of local commanders) for personnel permanently engaged on duties which include guarding.

c. Following the inclusion of amendments to the orders.

The record is to document the person's rank, number, name, signature and date of signature. The records are to be kept for a period of 12 months following the date of signature.

05839. Spare.

Patrols

General Principles

Consideration for Use

05840. COs/HOEs are to consider the use of security patrols, depending on the security category of the establishment, and the minimum baseline measures for the protection of protected material (see Section I) and the BIKINI alert state.

Arming of Patrols

05841. Patrols will be armed if armed guarding has been ordered by CinCs. DCDS(C) is responsible for issuing an Arming Directive which CinCs may further amplify.

Nature of Patrols

05842. The nature and extent of the patrols will depend on the other security measures that are in force within the establishment as part of the minimum baseline measures methodology. Where a large area is to be protected, 'beats' should be

considered to separate patrols, each responsible for its own area. In determining the tasks of the patrols, paragraphs 05812 and 05813 inclusive apply.

Patrol Procedures

Inside Buildings

05843. Guards patrolling inside buildings are to ensure the following:

a. **On the first round after cease work.**

(1) There are no intruders in any part of the buildings, the identity of all personnel is known and their right to be in the buildings is confirmed.

(2) All security containers are properly locked.

(3) No protectively marked documents/material/disks/waste have been left out.

(4) All doors and windows and any other possible means of entry are secure and intact.

b. **On subsequent rounds.**

(1) All containers are checked on a random basis.

(2) There are no intruders in the parts of the buildings visited.

(3) Checks are made that those doors, windows and other possible means of entry on the route of the patrol are secure and intact. They should be selected so that all are checked at least once every three rounds.

External Patrols

05844. External guard patrols are to carry out occasional patrols around buildings selected at random as follows:

a. **First patrol.** On the first patrol after close of work they should ensure that all buildings are properly secured and, at sites secured by a perimeter, that there are no intruders.

b. **Subsequent patrols.** On subsequent rounds they are to ensure that a check is made of the areas surrounding some of the buildings, selected on a random basis, so that all surrounding areas are checked regularly.

Timing of Patrols

05845. The timing of patrols is not to be made public and the guards themselves are to be warned of this. Guards are not to be aware of the exact timing of patrols until they come on duty.

Breaches of Security

05846. On each round they are to ensure that any breaches of security and incidents receive immediate corrective action and are recorded and reported to the establishment security staff. Any recovered protectively marked material is to be secured in an approved security container. The full procedures to be taken for breaches of security are laid down in JSP 440, Volume 1, Chapter 2.

Recording Action by Patrols

05847. In addition to the mandatory security check sheet which is signed by the occupant of a room, the following mandatory and optional recording action to record patrol activity applies:

a. **Mandatory.** The details of all security rounds are to be entered into a log or DOB. The details recorded are to show the buildings visited, times of the patrol, and rank(s)/name(s)/callsign of the patrol. Records are to be kept for 12 months. If mechanical or electronic patrol monitoring equipment is available the requirement for a written record may be dispensed with.

b. **Optional.**

(1) **Container and room check sheets.** In addition to the mandatory recording action described above, establishments can optionally position container check sheets in each room where protectively marked material is kept. The check sheet is signed by the patrol and the time of check of container(s) also entered on the sheet for each check out of hours. An example of such a form is at Annex A. Records are to be kept for 3 months.

(2) **Patrol recorder points.** Patrol recorder points (PRPs) can be sited in places where it is important for patrols to visit. Various methods of providing evidence of patrol activity are available e.g. Recorder points may require signing by the guard, a card 'clocked' or electronic information to be input by the guard to provide evidence of irregular patrol activity. Clocking records or logs are to be examined by the ESyO and where necessary, irregularities investigated. Records are to be kept for 3 months.

Dogs

Effectiveness and Deterrent

05848. Dogs are an effective intruder detection system when used to protect installations where there is little or no human traffic at night. They are a particularly effective deterrent to intruders.

Security Notice Boards

05849. Where guard or Service/MDP police dogs are in use on an establishment, appropriate warning signs are to be displayed at entrances and at regular intervals around the perimeter warning (or words to the effect that)

WARNING - RAF POLICE/POLICE/GUARD(as appropriate)
DOGS ON PATROL

In addition, standard pictorial warning signs (yellow triangle with a black silhouetted dog's head) are to be displayed at regular intervals around the perimeter. Units abroad are to have the signs in the local language.

Guard Dog Act 1975

05850. The use of guard dogs is governed by the Guard Dogs Act 1975 and advice is to be sought from Command security staff before their first use.

Rules of Engagement

05851. The Rules of Engagement for the release of dogs by Defence personnel on duty in the United Kingdom are contained in JSP 398, the Compendium of ROE, at Card C, and are reproduced at Annex B to this Section.

Additional Security Measures

Checks at Cease Work

05852. All rooms and compartments are to be checked by their authorised occupants before they are left vacant at cease work to ensure that all protectively marked material, including waste has been put away in security containers and that these are properly locked and all security keys mustered.

Room Security Check List

05853. A security check list showing that all security containers have been locked, windows closed, facsimile machines, photocopiers and computers secured is to be signed by the last person out of the area. A sample copy of such a check sheet is at Annex B to Chapter 4.

Clear Desk Routine

05854. Surfaces of desks and other office furniture are to be cleared of all papers, whether protectively marked or not, to facilitate security checks by both the occupier prior to leaving and thereafter by independent checkers.

Checks by the ESyO

05855. In addition to the patrol activity described in this part, surprise percentage checks are to be made by the ESyO out of normal working hours covering the internal and external security of offices, buildings and installations. Occasional checks of offices left unoccupied during lunch or other break periods are also to be made.

Action to be taken for Unsecured Protectively Marked Material

05856. The actions to be taken when unsecured protectively marked material is discovered by the guard force is to be detailed in their orders. Guidance is also given at Annex C to this Chapter.

This page intentionally left blank.

ANNEX A TO SECTION VIII

SECURITY PATROL ROOM CHECK SHEET

Mon/Yr	/	**Branch**		**Building**		**Room No**	

I have signed below to certify that:

a. All protectively marked material has been secured.

b. All security containers are locked.

c. All windows are security closed.

d. There are no apparent fire or other safety hazard.

Date	Ceasework		Independent checks					
	Check		Check 1		Check 2		Check 3	
	Time	Signature	Time	Signature	Time	Signature	Time	Signature
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								

18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								

ANNEX B TO SECTION VIII

GUIDANCE FOR THE

RELEASE OF DOGS BY SERVICE PERSONNEL ON DUTY

General

1. Dogs may be used to assist with a lawful arrest or to prevent crime following Rule 680. A dog must be used only in appropriate circumstances. The release of a dog for the purpose of apprehending a person must only be used as a last resort, other than the use of firearms, in the specific circumstances detailed below. Patrol Arm True dogs, which are used for special roles, are highly suited for this task.

Challenging

2. A challenge MUST be given before the release of a dog unless:

   a. To do so would increase the risk of death or injury to you or any other person;

   OR

   b. You or others in the immediate vicinity are under attack.

3. You are to challenge by shouting:

   "NAVY, ARMY, AIR FORCE, (as appropriate).
   HALT OR I WILL RELEASE MY DOG".

The Release

4. You are only to release the dog, should no other means be available to apprehend a person, if, on reasonable grounds you believe:

a. A person is committing or about to commit an act likely to endanger life (e.g. firing a weapon or placing an explosive device).

OR

b. You, the handler, come under attack.

OR

c. A person is causing injury to others.

OR

d. A person is threatening to cause injury to others.

OR

e. A person has just killed or injured someone or attempted or threatened to kill or injure someone.

OR

f. A person is breaking into an armoury or ammunition/explosives store or ammunition/explosives storage area.

OR

g. An unauthorised person is attempting to make off with arms, ammunition or explosives.

OR

h. It is necessary to do so to protect property, equipment or vehicles belonging to the Ministry of Defence, or in the care of MOD personnel, against serious acts of sabotage, theft or vandalism.

You may then release the dog using the appropriate command. Upon release, you are to follow the dog and order the person to stand still. When they are still, you are to command the dog to "leave", regain control of the dog and initiate the arrest procedure.

ANNEX C TO SECTION VIII
SEARCHING

Introduction

1. This document sets out the MOD's policy on searching, and is directed at non – police Guard and Security Forces, including Service personnel, MGS and civilian contract guard forces, on MOD property (MOD sites, establishments, premises and land) in Great Britain. In general, a search may be carried out only where a person consents to being searched. Members of a guard or Security force do not have any specific powers in relation to search. The Civilian Police Forces (CPF) and MOD Police (MDP) have certain other powers to carry out searches in other circumstances, either under the Police and Criminal Evidence Act 1984 (PACE), or under Scottish Law. The procedures and powers for searches carried out by Service police are set out in JSP 484 (Service Instructions for Search).

Reasons for Search

2. The reasons for a search may include:

a. On Entry to an Establishment. Searching may be conducted to prevent and deter terrorists or other extremists from seeking to gain access to attack an establishment or its occupants. It may also be conducted to prevent and deter unauthorised equipment, such as electronic or recording equipment, from being brought onto an establishment, thereby countering the espionage threat.

b. On Exit from an Establishment. Searching may be carried out to prevent and deter the illegal or unauthorised removal of property, including protectively marked material, from an establishment.

c. Within an Establishment. Exceptionally, other circumstances may arise where a search is required, for example where persons acting suspiciously are apprehended. This refers to the apprehension of intruders or individuals where there are reasonable grounds for believing that they may present a danger to the establishment, rather than those who are the subject of a crime related investigation.

MOD Policy on Searching

3. It is MOD policy that on MOD property all persons, their belongings and their vehicles are liable to be searched on entry, during their stay or when they leave MOD property, as stated in Vol 7 of the MOD Personnel Manual. It is recommended to Heads of Establishments that a record of searches be maintained. In circumstances of dispute, refusal to consent to be searched or upon making a find, a record must be made. An example of an appropriate form for use in such circumstances, that TLBs / Commands may wish to replicate, is at Appendix 1.

4. Everyone entering an MOD site is to be informed, or reminded, that they are liable to be searched. Notices to this effect are to be prominently displayed at any of the following: pass offices, entry points or guardrooms through which access is given to MOD property. An example of appropriate wording for notices is at Appendix 2. In addition, everyone potentially affected is to be informed that all personal effects left unattended and unsecured in offices or on MOD property are liable to be searched. Line managers are regularly to brief all persons working on MOD premises and land that this policy exists and practical methods of bringing this policy to the attention of all persons entering MOD property are to be considered, eg including it on passes issued to personnel.

5. If a person consents to be searched, then they may be searched either by Police (Service, MOD or civil), or by any member of the establishment Security Force. This Security Force may be Service Personnel, MOD Guard Service (MGS) or civilian contract guard force personnel.

Searches with Consent

6. It is a Condition of Service for MOD employees and a standard condition for contracted and subcontracted personnel that their person and belongings or transport on MOD property are liable to search. The Department therefore takes the view that they have given their implied consent to be searched at any time when on MOD property, including at the point of exit. Despite this, personnel are still to be asked to give their consent before being searched.

7. If a person does not consent to being searched on entry to MOD property, access may be denied; they themselves have the option not to enter MOD property if they object to searches taking place.

Searches without Consent

8. A person may refuse to be searched when asked, in which case a search without consent may not be undertaken unless the person carrying out the search is a member of the CPF, MDP or the Service Police, using one of the specific powers vested in them.

9. If it is suspected that a person within, or in the immediate vicinity of MOD property or premises, constitutes an immediate and substantive threat to life, they may be arrested and, if they still present a danger to themselves or others, they may be searched by any member of the establishment Security Force with or without consent.

Search Criteria

10. The term 'search' means the search of a person (the individual), their personal belongings (eg baggage) or their vehicles. This includes the search of unattended personal belongings on MOD property, for example briefcases or bags left in offices, or unlocked desk drawers.

a. Person searching.

(1) A search of a person may be conducted only by a member of the same sex, except where an immediate and substantive threat to life is believed to exist, and no member of the same sex is immediately available, in which case a search may be carried out by a member of the opposite sex.

(2) Only cursory searches involving the examination of outer clothing are to be carried out.

b. Personal belongings. A person of either sex may search personal belongings. However, if the owner is present and requests that a search be carried out by a member of the same sex, arrangements for this are to be made, provided a suitable searcher is readily available. If a suitable searcher is not readily available, the search may proceed only with the individual's consent, or if the search is carried out by a police officer with appropriate constabulary powers.

c. Vehicles. Persons of either sex may search vehicles.

Guidelines.

11. The need for training of personnel assigned to searching duties will vary, depending on the type of guard force and the categorisation of the establishment. As

a minimum, these personnel assigned to searching duties are to be made aware of the following guidelines:

a. Consent. Irrespective of the circumstances, all personnel are to be asked to give their consent prior to a search commencing.

b. Reasons for search. Those carrying out searches must be able to explain the reasons why they intend to carry out a search, as the person to be searched may well ask the reason. Searchers should be able to explain that the search is, for example, for security purposes (to deter or detect terrorists or espionage), or to combat and deter theft.

c. Use of force. The use of force will not normally be justifiable. Force may be used only by the CPF, MDP or the Service Police where they have the necessary powers. In circumstances where an immediate and substantive threat to life is believed to exist, personnel other than police officers may carry out a forcible search - but only as a last resort. Searching personnel are to be warned that the use of force when not justified, or an excessive use of force when use of reasonable force is justified, may expose the searcher to allegations of assault and possible criminal prosecution.

d. Searching techniques. Searches in public must be restricted to a superficial examination of outer garments, usually by running hands over the outside of a person's clothing. A person may be asked to remove an outer jacket, headgear or gloves voluntarily. A person may be asked to remove all items from their pockets; searching personnel **are not** to place their hands in any pockets.

e. Personal belongings. A search of personal belongings, for example a bag or a briefcase, may be carried out to ensure that it does not contain unauthorised material, or dangerous or prohibited items, such as an explosive device, a weapon, or protectively marked material. For instance, an unattended briefcase, left unsecured in an accessible cabinet or drawer, is liable to be searched. However searching does not extend to an examination of personal items such as diaries, personal papers or notebooks, beyond the point necessary to establish that the item is indeed personal, whereupon the examination of it is to stop. Thus studying such material to look for passwords, combinations or other compromising material is unacceptable. This applies to all personal belongings, whether they be accompanied by the owner or left unattended and unsecured elsewhere.

f. Action upon making a find. Guards who have no constabulary powers should, on finding something suspicious, including MOD property being removed without authorisation:

(i) Ask the person for an explanation and, if unsatisfied with the response, ask the person to wait while the police are called to investigate.

(ii) If the person refuses to offer an explanation or refuses to wait, guards should not detain them but should report the matter immediately and if necessary summon police assistance. .

(iii) Should something be found that a guard believes may constitute an immediate threat to life, for example a weapon, the guard may detain that person by using citizens' powers of arrest. CPF, MDP or Service police should be summoned immediately.

(iv) Should an unattended item be found in a room, its presence there indicating a breach of security, then that item may be locked away and the person responsible for it notified of where to find it.

(v) In all cases, guards should consider the need to preserve evidence and should handle an item only if it is necessary to do so to prevent further danger, or prevent the continuation of a breach of security.

g. Instigation of, and selection for Search. Entry and Exit searches will ordinarily be instigated by the Commanding Officer of the unit or by the HoE. Where searching is conducted for deterrent value and not in response to threat or specific information, personnel and / or vehicles are to be selected for searching in an entirely random manner.

Searching Policy Overseas.

12. The principles of this policy apply equally to overseas establishments, in that the underpinning tenets are; the reasoning behind searching, the jurisdiction within which to search, and consent to search. The question of jurisdiction is a key issue and must be verified locally, taking account of regional cultures and laws. The powers of establishment security forces may well be different overseas, depending on their composition and status (eg where locally recruited staff are employed). MOD personnel on bases abroad will be subject to searching as if they were in the UK.

Clarification

13. Legal advice should be sought in any case of need for clarification, or in any case of uncertainty regarding this sensitive and potentially contentious subject.

This page intentionally left blank

APPENDIX 1 TO
ANNEX C TO SECTION VIII

RECORD OF SEARCH **All details to be printed**

DATE: _____ **LOCATION:** _____

INDIVIDUAL CONDUCTING SEARCH:

Name	
Service / ID number	
Parent organisation	
Male / Female *	

SUBJECT OF SEARCH:

Name	
Service / ID number	
Parent organisation	
Male / Female *	

Do you consent to a search*? **Yes** ☐ **No** ☐

Searched*: **Person** ☐ **Baggage** ☐ **Vehicle** ☐

Signature of Individual searched: _____ **Time:** _____

Comment (*if individual wishes to comment)*: _____

_____

_____

Signature of Searcher: _____

Signature of witness: _____

*Indicate as appropriate** *(if present)*

This page intentionally blank.

APPENDIX 2 TO ANNEX C TO SECTION VIII

Appropriate wording for advertising a liability to search whilst on MOD property:

All persons wishing to enter this site/establishment/building are to be aware that they, their possessions or vehicles are liable to search at all times. This includes on entry, whilst in the site/establishment/building* or when leaving.*

*Delete as appropriate

This page intentionally blank.

SECTION IX TO CHAPTER 5

CONTROL OF ENTRY

Pass Systems and General Regulations

This Section is being completely revised by D Def Sy and will be the subject of a Defence Council Instruction published in Oct 01 and issued in a DSO Guidance Note.

Paras 05901 – 05969 under review.

This page intentionally left blank.

SECTION X TO CHAPTER 5

AUTOMATIC ACCESS CONTROL SYSTEMS (AACS

Introduction

General

051001. This section deals with policy concerning the installation, effective use and management of automatic access control systems (AACS) within the Defence estate.

The Principle of AACS

051002. The principle of AACS is that entry to a building, or area within a building, is controlled by the use of a card/token and Personal Identification Number (PIN), carried and known only by authorized personnel which, when used together, activate an access barrier.

Use of AACS

051003. Establishments are to be encouraged to consider the security benefits that may be achieved by the installation of AACS to buildings or zones within buildings. The benefits may be most applicable to establishments located in a single building in an urban area where an AACS system could provide increased efficiency in controlling access and a reduction in the guard force. Such a reduction may provide significant long term cost savings.

051004. Further information, advice and guidance. Further information, advice and guidance can be obtained from the following sources:

a. Where establishments are considering installation of an AACS system, consult TLB PSyA security staff to provide specialist advice and appropriate policy input (eg. AACS readers should be compatible with Watermark® technology used in the current version of the Defence Identity Card (DIDC)). Section II provides information and direction on procurement of major security equipment and systems. In addition, where such work constitutes a works service project, the procedures detailed in Chapter 5 Section II Annex A are to be adhered to.

b. Advice on the completion of an operational requirement (OR) is also to be sought from TLB PSyA staff.

c. See Section IX for more information on ID Cards and AACS.

051005. Requirement for TLB PSyA approval. Whilst the initial decision on the requirement for a AACS is taken at establishment level, it is essential within the Defence estate that the quality of system ultimately procured for the establishment is of an acceptable standard and design. This is achieved by the involvement of TLB

PSyA staffs monitoring and approving ORs from establishments to ensure that appropriate standards are maintained throughout the Defence estate.

Responsibility for AACS

051006. The following responsibilities are as shown:

a. **Central policy.** D Def Sy is responsible for the issue of central policy on the design and types of AACS to be installed within the Defence estate. D Def Sy is advised by the Defence Identity Card and Access Control Working Group, a working group of the Security Policy Advisory Group.

b. **Installation.** The installation of AACS is the responsibility of the TLBs implemented through the normal works project or property management chain.

Operational Requirement

051007. It is essential that before any purchasing action is commenced, establishments define clearly what they expect an AACS to do by preparing an OR. The OR is to specify the following:

a. The area/building in which the AACS is to be installed.

b. Any manpower considerations and/or savings.

c. Whether linkage to CCTV/VMD or IDS is required.

d. Proposed monitoring requirements.

e. Any other performance requirements.

Special Note: Within MOD, AACS must at present, use a PIN and 'Watermark'.

Site Survey

051008. Following approval of the OR, a site survey is to be arranged by TLB PSyA security staff (who may task their single-Service security organisation, and/or SSG).

Audit of System

051009. An audit of the IDS system is to be carried out by professional security staff in accordance with the direction given at Section II to this Chapter, para 05210.

Definitions

051010. The following definitions apply:

a. **AACS.** An electronic system which can restrict entry/exit from a controlled area.

b. **Controlled area.** An area which may be entered after the presentation of valid recognition data.

c. **Access control point (ACP).** The place at which access is controlled by a guard, door, booth, turnstile or other barrier.

d. **Token.** A device containing encoded recognition data, which may include biometric detail of an individual; a token in the Defence estate is usually an ID card, pass or permit.

e. **Keypad.** A data entry point for the input of a code into an AACS.

f. **Personal identification number (PIN).** A sequence of characters allocated to the user of a keypad. A PIN must never be portrayed on a token.

g. **Reader Unit.** Equipment for the extraction of recognition data from a token.

h. **Local control unit (LCU).** A device which processes recognition data to enable a usable output.

i. **Central control unit (CCU).** Equipment directing and monitoring the functions of 2 or more LCUs.

j. **Trigger.** The use of a token to actuate a secondary AACS. A secondary system is the electronic version of the "Tally or Exchange pass".

Classes of AACS

051011. The Classes of AACS are described at para 05119.

Types of AACS

051012. There are 3 types of AACS, namely:

a. **Hands on.** This requires the bearer of a token to use it physically as an item of equipment.

b. **Proximity.** A proximity (hands free) is one where the bearer carries a passive/active radio/infra-red token which uses a coded signal to release the barrier.

c. **Biometrics.** This is where identity is checked by some physiological feature offered at the point of entry against the record of the same feature

held in a computer memory. In general, intrusive/active physiological feature reading such as retina scanning should be avoided.

051013. In higher security installations it is mandatory for a PIN to be used if a "hands free" system is in place. It is policy for "hands on" systems only to be used

within the MOD estate for personnel; "hands free" systems may be used for vehicles. Biometric systems are not to be installed without the prior approval of the appropriate TLB PSyA and D Def Sy.

Installation Criteria

051014. When considering the installation of an AACS, a study of the minimum baseline measures is necessary. Whenever it appears that a substantial saving in manpower or a marked improvement in protective security will occur then AACS should be considered for installation. The advantages and disadvantages which should be considered in relation to the proposed installation are as follows:

a. **Advantages.** The advantages of AACS are:

(1) Continuous controlling of entry even in the absence of guards.

(2) Cannot be distracted, suborned, persuaded or threatened.

(3) Installation expenditure is a one-off outlay.

(4) Upkeep and maintenance costs are low.

(5) Can be programmed to detect unauthorised users.

(6) Provides a barrier against forced entry.

(7) Gives protection to guards operating the system.

(8) Will maintain a record of token holders' movements.

b. **Disadvantages.** AACS has the following disadvantages:

(1) Human supervision is still needed for visitors, trades people, breakdowns, etc.

(2) Collusion by unauthorised and authorised persons cannot be prevented.

(3) Controls entry/exit only; does not safeguard protectively marked material.

Security Criteria

051015. Where an AACS is installed to control direct access to an area housing protectively marked material it is to comply with the following:

a. Have a standby source of power.

b. Have a "fail shut" device which ensures that the area to which the system gives access is secure in the event of a failure or emergency.

c. Be fitted with a mechanical override on the secured side of the barrier to permit exit in an emergency.

d. Be fitted with security locks for use when shut down.

e. Be proofed against manipulation or tampering.

f. Be fitted with an alarm to signal failure or abuse of the system.

g. Be able to reject tokens which are notified as invalid.

h. Be able to lock out a PIN using token after 3 unsuccessful attempts at entry.

i. Prevent tailgating and passback.

System Security

051016. When a AACS has been installed its reliability and security must be maintained by good management, supervision and regular servicing. This includes:

a. Ensuring that access to the computer and its software is restricted to authorized personnel.

b. All cards lost, stolen or no longer required should be programmed out of the system as quickly as possible.

c. Consideration is to be given to making special arrangements, such as withdrawing cards or programming them out of the system, for staff who, for a prolonged period, are on leave, sick leave, detached duty or abroad.

System Security Policies and Security Operating Procedures

051017. Where AACS are computer-controlled, appropriate system security policies (SSPs) and security operating procedures (SyOPs) must be issued for the system.

System Criteria

Incorporation of Watermark® Technology

051018. An increasing number of establishments are installing or planning to install AACS. It is MOD policy that new systems should be compatible with Watermark® technology. In addition, to being a tried, tested, approved and secure technology, Watermark® systems can utilise the Tri-Service Defence ID card (DIDC) and permanent passes manufactured using Site Access Management Systems. This limits the number of cards carried by an individual on an establishment. Accordingly, Sector Security Authorities need to ensure that establishments install only Watermark® compatible systems (the use of Special Services Group for system surveys should ensure that this requirement is complied with).

Watermark® Specification

051019. Copies of the Watermark® specification can be obtained from SSG. The names of approved 'Systems Houses' can also be obtained from SSG.

Effective use

Components

051020. There are 3 components which together determine the effectiveness of an AACS, namely:

a. The barrier which permits access.

b. The token which is used to seek admittance.

c. The control unit which accepts or rejects the token and orders the barrier accordingly.

Barriers

051021. Barriers for the admittance of personnel can be doors, turnstiles or booths. They are classed as "higher" or "lower" security installations.

Higher Security Barrier

051022. Where monitoring of an ACP is from a distance, a higher security barrier is to be installed. This involves a structure allowing no space between barrier and ceiling/roof or adjoining walls/fences; entry is to be restricted to one person at a time and extra precautions, such as weight sensors or metal detectors, are to be incorporated if the assessed threat determines the need.

Lower Security Barrier

051023. Where 'on site' monitoring of an ACP occurs, a lower security barrier such as waist high turnstiles, may be used; this class of barrier is suitable for use at a permanently manned ACP.

CCUs and LCUs

051024. Where more than one ACP is to be used to access a location, a CCU must be provided; it is not acceptable, except in very special circumstances which are approved by the TLB PSyA, for unconnected LCUs to admit access to the same location.

Siting of LCUs and CCUs

051025. LCUs and CCUs are to be sited within the protected area unless encrypted communications are provided. LCU/CCUs are to be housed in RESTRICTED areas under the supervision of the ESyO. Battery power for data storage at LCUs should have an 8 hour and for CCUs a 12 hour endurance. Batteries must be capable of being fully recharged within 8 hours.

LCU Records

051026. An LCU must be able to record the following:

a. Times of events.

b. All entries and exits.

c. Entries denied with the reason.

d. Any alarms actuated.

CCU Capability

051027. In addition to the records required of an LCU, a CCU must be able action the following:

a. Store all PINs in use and be able to accept updates at intervals not exceeding 12 hours.

b. Provide a correlation of PINs with users to specified system managers.

c. Store sufficient information to provide an audit trail of user events, including alarm records, for a minimum of one week.

Management

051028. System manager. Every AACS is to have a system manager and deputy with requisite support personnel nominated. The system manager and deputy are to:

a. Be appointed by the HOE and receive written instructions regarding their duties.

b. Be responsible to the ESyO for overall supervision of the system.

c. Control the issue of token access and PINs, including the validation and deletion of access right.

d. Examine system logs on a regular basis.

e. Investigate all alarms and malfunctions.

f. Have faults attended to at once.

g. Ensure that only they have access to the programming facilities of the system.

Servicing of System

051029. The reliability of an AACS depends on regular servicing and correct use. The system manager is to ensure that operating and maintenance staff receive adequate training before the system commences operation and before system updates occur.

Maintenance Contracts

051030. Establishments are to ensure that an effective maintenance contract is in place through the life of the system which allows for repair to the system to be actioned within 24 hours of the system failing.

Doors

051031. An AACS may be considered for use in conjunction with a conventional door (for example, to restrict access to a room or area inside a building). However, the level of security provided is dependent on the security standard of the door. A door is more vulnerable to being circumvented than a properly designed barrier, particularly by tailgating, therefore a strong adjustable door closer is to be fitted.

Secondary systems

Biometric Systems

051032. Biometric systems verify a user's identity by checking some physiological feature offered at the point of entry against the record of the same feature held in the computer database. Biometrics systems are currently under trial by D Def Sy. An approved list of systems will be issued in due course.

Advantages and Disadvantages of Biometric Systems

051033. The main advantage of a biometric system is its verification of the identity of the person rather than the token. Disadvantages are the relatively high installation costs and, sometimes, the high level of sensitivity needed to guarantee prevention of unauthorized entry; this can result in a large proportion of authorised users being denied access. It is for these reasons that all systems need to be approved by the centre.

SECTION XI TO CHAPTER 5

SECURITY CONTAINERS AND SECURE ROOMS

Security Containers

General

Level of Protection

051101. Protectively marked material is to be given a level of direct protection appropriate to its value so that those without authority do not gain access to it. The first line of protection is a container or room.

Further Information, Advice and Guidance

051102. The following information, advice and guidance on security containers can be obtained:

a. All personnel with a responsibility to safeguard protectively marked material should refer to the minimum baseline measures of physical security (Section I) for guidance in applying appropriate protection.

b. Chapter 3 concerning risk management should be consulted in conjunction with this part.

c. PSyAs may be contacted to advise on the application of the minimum baseline measures matrix, risk management and any additions to the list of approved containers.

d. Section I Annex E provides a summary of security equipment and security measures including a full listing of all the Classes of security equipment.

e. Section XII concerning locks and security keys.

f. Chapter 4 concerning document security.

Approved Containers

051103. Approved containers are designed to provide resistance to surreptitious attack and are allocated to a Class (1 to 4) according to the degree of protection they offer (Class 4 offering the highest level of protection and Class 1 the lowest). A measure of protection against forcible attack is, in addition, offered by containers in Classes 4 and 3. Containers used to house protectively marked material are to be fitted with an appropriate lock (see Section XII of this Chapter).

Classification of Containers

051104. Containers are classified according to the level of protection they offer from both forced and surreptitious attack. A list of classifications is at para 05114. Security Equipment Assessment Panel (SEAP) approved containers are listed at Section I, Annex E.

Standards

Responsibility for Standards

051105. SEAP is responsible for producing the standards for assessing the quality and level of protection offered by security containers.

Specialised Storage Requirements

051106. Where specialised storage requirements cannot be met by a container in the existing range advice is to be sought from PSyAs.

Modifications

051107. Establishments are not to modify or design their own security containers. Requirements for a new type of security container are to be staffed through PSyAs who will assess the requirement prior to consulting DDef Sy for assessment and approval.

Assessment of Commercial Containers

051108. PSyAs may carry out their own assessment of commercial containers to meet a Class 1 requirement (consulting D Def Sy if necessary). The standard is given in the Handbook of the Manual of Protective Security. The standard will be used to assess the suitability of commercial containers according to Defence needs. Details of items for consideration as Class 1 security containers are to be forwarded to DDef Sy through PSyAs.

Care of Security Containers

Surface Finish

051109. The surface finish on Class 2 to 4 security containers has been specially selected. When damaged in a surreptitious attack it is difficult to restore without leaving discernible traces. Establishments are not to arrange for containers to be repainted or resprayed other than to the original standard. This standard of repainting cannot be carried out on site and it is necessary to arrange for the work to be done in a properly equipped factory facility. Details of security container refurbishing is included in the Handbook of the Manual of Protective Security or as provided by PSyAs by way of security instructions for container refurbishment.

Comments

051110. The following other precautions are to be taken with containers:

a. Holes are not to be drilled in the body of security containers of Classes 2 to 4. This does not apply to containers that incorporate design features to allow then to be drilled and bolted to the floor, such as approved document chests. Holes may be drilled in the body of security containers for the purpose of fixing to walls or floors but this may limit their future use as security containers once removed from their fixings when they become Class 1 only.

b. Attachments are not to be fitted to containers which might be used by an attacker to camouflage a surreptitious attack.

c. Labels or notices are not to be stuck to the outside of security containers.

Control of Security Containers

Numbering of Containers

051111. Every container is to be allocated a number by the ESyO and a record kept of its history that show:

a. Location of the container.

b. Details of any repairs and maintenance carried out on the container.

c. The unique number of the lock on the container.

Disposal of Security Containers

051112. When returning or disposing of security containers the following action is to be carried out:

a. A thorough check is to be carried out to ensure that all protectively marked material has been removed. Particular attention should be paid to filing cabinets where checks should be made that material has not fallen down the backs of drawers or into the base of the container.

b. Prime responsibility lies with the person handing over the container. On completion of the search, a MOD Form 425 (Certificate of Inspection) is to be signed and attached stating:

' I CERTIFY THAT I HAVE SEARCHED CONTAINER (SER NO...) AND ALL OFFICIAL PAPERS AND EQUIPMENT HAVE BEEN REMOVED.'

A locally produced certificate may be used in lieu of MOD Form 425.

c. Containers that are fitted with combination locks are to have their number reset to the manufacture's number.

Full instructions for the disposal of furniture are contained in JSP 384.

Review of Security Containers

051113. Holdings and usage of security equipment are to be reviewed at no less than annual intervals to maximise the economic use of the equipment.

Easily Removable Containers

051114. Security containers which can be removed without difficulty can be secured to a wall or floor (NB. In ships, all security containers are securely fixed to the ships structure). Fixings are to be arranged so that the container conceals them and renders them inaccessible.

Key Boxes

051115. Key boxes are not to be fixed to plasterboard partition walls**.** If there is no firm fixing available, e.g. into brick or concrete, key boxes are not to be used and keys are to kept in other appropriate security containers. Holes are not to be drilled in other containers for the purpose of fixing a key box to them.

Container Records

Mandatory Information

051116. The following mandatory information is to be displayed inside the container:

a. Date of last combination change.

b. Signature and details of person affecting combination change

c. Date next combination change due.

d. Address and contact telephone number of custodian in case the container is found open.

Additional Information

051117. Where so required, the following information can be displayed inside the container:

a. List of permanent musterable items.

b. Priority of destruction of material in an emergency.

c. Fire preparedness plan.

Action in the Event of Suspected Tampering

Immediate Action

051118. The following action is to be taken in addition to any administrative action required under the provisions of Queens Regulations:

a. The suspected tampering is to be reported immediately to the ESyO who is to inform the head of establishment without delay.

b. When the circumstances are suspicious the appropriate security unit is to be requested to investigate following consultation with PSyAs. The suspected theft of protectively marked documents and the collection and preservation of physical evidence are matters which should involve the Service police jointly with the relevant security organisation.

c. As further handling may destroy evidence, the container is to be preserved for examination by the investigator.

d. Whenever there is reason to suspect compromise of any or all of the contents, immediate action is to be taken under the provisions of Chapter 2.

e. DDef Sy is to be informed, by the PSyA, where appropriate in accordance with the policy at Chapter 2. If espionage is suspected and it is perceived that there is a need to inform Ministers, PSyA advice is to be sought without delay.

Secure Rooms

General

Introduction

051119. Where there is a need to house large quantities of protectively marked material, it may be convenient and economical to store the material on open racking in a specially protected room. The room is to be designed to offer the same level of protection as the security containers it replaces.

Further Information, Advice and Guidance

051120. Further Information, Advice and Guidance is available as follows:

a. Establishments considering the conversion of such rooms are to seek advice and obtain approval from their PSyA prior to detailed planning at establishment level begins.

b. Detailed advice on structural standards for rooms can be obtained from SSG via PSyAs.

c. Details of SEAP approved locks and security doors quoted in this section can be found in the Catalogue of Security Equipment: A summary of the approved equipment is at Annex E to Section I.

d. Implementation should be via the property management system, except for some programming of software aspects.

Classes of Room

051121. The Classes of room identified as suitable for use instead of security containers of Class 2 to 4 are described at para 05116. The rooms by type are shown at Section I, Annex E.

Choosing a Room

Considerations

051122. When considering which type of room to construct the following is to be considered:

a. The quantity and protective marking of the material to be housed.

b. The level and type of threat and whether protection against a surreptitious or forced attack is needed.

c. The extent of control which may be exercised over the accommodation adjacent to, above and below the room.

Types of Room

051123. Where a room is used as a security container, ie protectively marked material is kept therein without security furniture, the standards below apply.

Strongrooms

051124. A strong room giving protection equivalent to a Class 4 security container is of permanent construction, is an integral part of a building, and has only one point of entry fitted with a combination locked strong room door. Its floor, walls and ceiling are otherwise unbreached and constructed of ferro-concrete. Advice on construction details can be obtained via Command security staff.

Secure Rooms

051125. A secure room is designed to afford the same level of protection as the security containers it replaces. There are three types of secure room designed for the storage of protectively marked material. Types A and B are designed to combine

protection against surreptitious attack with a measure of protection against forcible attack, and may be used for the storage of protectively marked material on open racking on non-approved containers. Type C has been devised to protect protectively marked material held on certain fixed disk computer systems and electronic equipment against surreptitious attack. The level of security provided by a type C secure room is less than that provide by a type A or B room and for this reason is not approved for the storage of protectively marked documents. Command security staff should be consulted before considering the use of a type C secure room. The details of secure rooms are at Annex A; detailed specifications can be obtained from SAFE/SSG via Command security staff. A secure industrial type building adapted for the purpose in accordance with the standard drawing will also qualify as a secure room.

a. **Construction.** Exterior walls, party walls, floors and ceilings should not normally form part of the Room. There should ideally be only one entrance, and any ventilation or cable ducting should be adequately protected against unauthorised access. If emergency exits are necessary they should be fitted with approved doors, emergency exit devices and wired into any installed intruder detection system, to the same standard as that required for the Room.

b. **Access to Secure Rooms.** Guards, cleaners and maintenance staff are not to be permitted unsupervised access to strong or Secure Rooms. The door to a Secure Room which is not in use or under close supervision is to be kept locked.

Locked Room

051126. A locked room is any room or office that can be locked (when left unattended) and will offer a degree of protection to its contents. All material protectively marked CONFIDENTIAL or above must be stored in approved security containers in locked rooms subject to the provisions of para 05248.

This page intentionally left blank

ANNEX A TO SECTION XI TO CHAPTER 5

SECURE ROOMS

Standard Type A Secure Room

1. **Introduction.** There should be only one entrance in Type A Secure Room, but if emergency exits are necessary they must be fitted with approved doors and emergency exit devices and be wired into any installed intruder detection system. Windows are not permitted. Air vents and ducts must be fitted with steel grilles or bar sets. Protectively marked material may be held on open racking or in non-SEAP approved containers in a Type A Secure Room. A lightweight version of the Type A Secure Room is available for use when the standard structure is too heavy for the building.

2. **Specification.**

   a. **Walls.** 150mm (min) reinforced concrete or in existing buildings, 340mm solid brick, cement rendered on both sides.

   b. **Floor and roof.** 150mm solid reinforced concrete.

   c. **Door.** Oxford or Cambridge door.

   d. **Lock.** Medway Locking unit or Fraser Bar, for emergency exists.

Lightweight Type A Secure Room

3. **Introduction.** The lightweight Type A Secure Room is designed for use where the standard Type A specification structure would be too heavy for the building. It can also be used in buildings to upgrade existing walls to a Type A standard. Windows are not permitted in a Type A Secure Room. When upgrading an existing building, windows must be bricked up or fitted with bar sets and covered with the lightweight structure.

4. **Specification.**

   a. **Walls.** A double sandwich of 18mm plywood, expanded metal (XPM) - 2073F and plasterboard finish, constructed each side of a timber studding framework.

   b. **Floor and roof.** Layers of plywood and XPM – 2073F, furnished to the required standard may overlay existing floor and ceiling which do not reach the required standard.

c. **Door.** Cambridge door.

d. **Lock.** Medway locking unit or Fraser bar, for emergency exits.

Standard Type B Secure Room

5. **Introduction.** There should be only one entrance in a Type B Secure Room, but if emergency exits are necessary, then they must be fitted with approved door and emergency exit devices and be wired into any installed intruder detection system. Windows should be bricked up or protected by fixed steel grilles or bars, as should air vents and ducts. Protectively marked material may be held on open racking or in non-approved containers in a Type B Secure Room. A lightweight version of the Type B Secure Room is available for use when the standard structure is too heavy for the building.

6. **Specification.**

a. **Walls.** 225mm brick or 200mm dense concrete block, cement rended inside and out.

b. **Floor and Roof.** 100mm (min) solid reinforced concrete.

c. **Door.** Ashford.

d. **Lock.** Medway locking unit, Fraser bar for emergency exit.

Lightweight Type B Secure Room

7. The Lightweight Type B Secure Room is designed for use where the standard Type B specification would be too heavy for the building. It may also be used to upgrade the standard of walls in an existing building to meet the required specification.

8. **Specification.**

a. **Walls.** A sandwich of 18mm plywood, XPM – 2073F and plasterboard finish constructed each side of a timber studding framework.

b. **Floor and Roof.** Layers of plywood and XPM – 2073F finished to the required standard may overlay existing floor and ceiling which do not meet the required standard.

c. **Door.** Ashford.

d. **Lock.** Medway locking unit, Fraser bar for emergency exit.

Standard Type C Secure Room

9. **Introduction.** A Type C Secure Room has been designed to protect protectively marked information held on fixed disc computer system and certain electronic equipment against surreptitious attack. There should be only one entrance but if emergency exits are necessary, then they must be fitted with approved doors and emergency exit devices and wired into any installed intruder detection system. Windows should be bricked up or protected by fixed steel grilles or bars as should air vents and ducts. Material protectively marked CONFIDENTIAL and above may **NOT** be held on open racking in a Type C Secure Room, but must be stored in approved security containers. A lightweight version of the Type C Secure Room is available for use when the standard structure is too heavy for the building.

10. **Specification.**

a. **Walls.** 112mm brick or 100mm dense concrete block, cement rendered both sides.

b. **Floor and Roof.** Any reinforced concrete slab.

c. **Door.** Croydon.

d. **Lock.** Any Class 2 lock or approved emergency exit device.

Lightweight Type C Secure Room

11. **Introduction.** The lightweight Type C Secure Room is designed for use when the standard Type C structure is too heavy for the building. It may also be used to upgrade the standard of walls in existing buildings to meet the required specification.

12. **Specification.**

a. **Walls.** A sandwich of 18mm plywood, XPM – 2073F and plasterboard finish fixed to the outside of a timber studding framework.

b. **Floor and Roof.** Existing solid floor and ceiling.

c. **Door.** Croydon.

d. **Lock.** Any Class 2 lock or approved emergency exit device.

This page intentionally left blank.

SECTION XII TO CHAPTER 5

LOCKS AND SECURITY KEYS

Locks

General

Introduction

051201. Security locks used for the direct protection of protectively marked material at levels of CONFIDENTIAL or above are to conform with SEAP approved standards. For the purpose of assessing and countering security risks, security locks are classified according to the level of protection they offer; Class 4 being the highest security and Class 1 the lowest.

Further Information, Advice and Guidance

051202. Full details of SEAP approved locks are contained in the Catalogue of Security Equipment (CSE).

Classification of Locks

051203. The classification of locks is shown at para 05115. SEAP approved locks are listed at Section I, Annex E.

Combination Locks

Operating Principle

051204. Combination locks which operate on the principle of rotating tumbler wheels generally offer a greater degree of protection against surreptitious attack than key locks.

Overlooking

051205. Security containers fitted with combination locks are not to be sited where there is a possibility that the dial of the lock can be overlooked by unauthorised persons (this includes siting containers away from windows where telephotography may be a threat). Where it is not possible to change the position of a container vulnerable to overlooking, dial masks are to be fitted to the lock.

Initial Supply

051206. Locks are supplied set on the manufacturers setting. When received, they are to be safeguarded and there is to be no unauthorised access to them.

Recording of Settings

051207. The following applies to the recording of combination settings:

a. Settings are to be committed to memory and are not to be recorded (even in cryptic form) except as per para 051207b below.

b. The setting of a combination lock is to be written down for emergency use and that record wrapped in metal foil laminated or opaque paper. The wrapper is then to be placed in a sealed envelope marked on the outside with the following information:

(1) Brief details of the related security container and location.

(2) The names and titles of the custodian and other persons authorised to have access to the written record.

It is best practice, but not mandatory, for the envelope to be protectively marked to the same level as the highest protective marking of the material held in the container itself. The user of the container is to sign across the flap and add the date after the envelope is sealed. The signature and flap are then to be oversealed with clear cellulose tape of at least 19mm width. The duplicate combination is to be passed to the ESyO, or in special circumstances the HOE, for safe custody.

Selection of Numbers

051208. When choosing combinations, the following are to be observed:

a. Combination settings are to be chosen only after reference to the manufacturer's operating instructions issued with the lock.

b. The numbers should be selected at random however if, for reasons of convenience eg in a registry, a mnemonic is necessary, it is to be of a kind which cannot be easily deduced i.e. not a telephone or obvious number.

Scrambling of Lock

051209. Combination locks are to be fully scrambled whenever a container is closed by turning the dial anti-clockwise at least five times.

051210. *Spare.*

Changing Settings

051211. The setting numbers are to be changed in the following circumstances:

a. When a container first comes into service or is taken over by a new user.

b. Every 6 months.

c. If a setting is known or thought to be compromised.

d. Whenever a lock has been repaired, serviced or inspected by a person who does not have authorised access to the contents of the container to which it is fitted.

e. When one of several persons who has access to a single container ceases to have authorised access eg on posting.

Manifoil Combination Locks (MCL) not in Use

051212. Security containers with MCLs that are not in use and that are not being returned to the manufacturer or disposed of are **NOT** to be locked on the manufacturer's combination setting. The ESyO can select one standard combination for all out of use containers and the record of the setting(s) are to kept by the ESyO at protectively marked SECRET level. The regulation for containers being returned or for disposal is at para 051112.

Vulnerabilities of Combination Locks

Attack Techniques

051213. Combination locks are vulnerable to a number of surreptitious attack techniques. All Class 4 locks will offer a degree of protection against an attack by drilling and manipulation; however personnel are to be aware of the potential threat of the following types of attack:

a. **Use of fingerprints.** Fingerprints of thumb or finger which, if aligned, will give an indication of the combination setting, may be left on the dial and bezel ring if the finger or thumb of one hand is used to steady the dial while the other hand is turning the knob. Those personnel who use this method of opening combination locks are to be encouraged to open them using one hand. Alternatively dial masks can be fitted to the locks.

b. **Rigging.** Rigging is possible if access can be gained to the back of the lock when in the unlocked position. Specially prepared parts can be substituted so that an attacker will be able to open the lock at will, regardless of its setting, while the authorised user will be unaware of any change in the lock. For this reason the following safeguards are to be observed:

(1) The manufacturer's setting is to be changed immediately the container is received by the user.

(2) Unauthorised persons are not to be permitted access to a container and its lock.

(3) The locks on security key boxes sited in corridors are to be fully scrambled at all times.

(4) Combination locks held as spares are to be stored under secure conditions by the ESyO.

(5) Locks despatched to addresses in the UK by normal channels should bear no description of the contents on the outer cover.

(6) A faulty lock is to be serviced only by approved Service personnel or an approved civilian locksmith.

c. **Radiography.** Radiography is a sophisticated attack which if access can be gained to both sides of a container, or door fitted with a combination lock, may reveal the combination setting.

Action in the Event of a Malfunction

051214. If a combination lock fails to open, personnel are to report the fact to the establishment security staff who will take appropriate action to rectify the situation. Non-security personnel are not to attempt to gain entry using tools.

Action in the Event of Suspected Compromise

051215. In the event of suspected compromise to a combination, the measures detailed at para 051238 are to be followed.

Maintenance and Repairs

051216. Repairs to combination locks are only to be carried out by an approved locksmith or trained members of security units and all transactions involving locks are to be carried out by the establishment security staff under the provisions of JSP 384. When the services of a UK locksmith are required overseas, authority is to be obtained from the relevant PSyA.

051217. Sites located in remote areas, or where a high level of security must be maintained, are advised to hold a limited supply of new or rebuilt locks, for use in emergency.

Vulnerabilities of Key Locks

Surreptitious Attack

051218. Key locks are vulnerable to surreptitious attack because they have a keyway into which probes and picks can be inserted, and a key which can be compromised or lost.

Selection of Door Lock

051219. When selecting a lock for fitting to a door it is important to consider where the lock will be used i.e. internally or externally, the type and size of the door it will be used on, the state of the door, hinges and frame.

Selection of Lock Mechanism

051220. When selecting the lock mechanism which will be the most appropriate, the following principles apply:

a. Single-sided locks are more secure than double-sided locks, although the incorporation of a throw lock does not detract from the security of a single-sided lock..

b. Mortice locks, which rely for strength on the door surrounding them, are not suitable for use on doors of less than 44mm thickness.

c. Rim locks depend for their strength on the nature of the fixings to the door.

Degree of Security

051221. A lock cannot offer any higher degree of security than the door to which it is fitted. It is pointless to fit an approved lock to a door which is weak or ill fitting.

Security Keys

Definition

051222. Security keys are those which operate locks fitted to:

a. Security containers used to house protectively marked material.

b. Doors of secure buildings, rooms or areas.

c. Security containers (boxes, pouches, briefcases etc) used for the transmission of protectively marked material.

d. Doors of rooms given special protection (i.e.'swept') against technical eavesdropping.

e. Armouries and ammunition stores.

Unauthorised Persons

051223. Keys can be easily copied from an impression, a photograph or a radiograph. Unauthorised persons are not to be given the opportunity to handle or examine security keys.

Security of Security Keys

051224. The security of security keys is to be maintained as follows:

a. They are to be issued against signatures in a key register to authorised members of staff.

b. The daily issue of keys is to be recorded in a key register

c. The number of keys issued for any lock is to be kept to the minimum.

d. A record (master key register) is to be maintained by establishment security staff or by branches, showing the following:

(1) The location of each key, together with a record of the lock to which it belongs.

(2) The date the working key (but not the duplicates) was signed out to the custodian.

(3) The identifying features of each key i.e. type registered number and number of duplicates.

(4) The printed names and ranks of the persons allowed to have access to the key.

e. The keys are to be mustered by the establishment security staff, at intervals not exceeding six months. They are also to be subject to spot checks. A certificate showing the results is to be rendered to the HOE.

f. When used to directly protect material marked CONFIDENTIAL and above, the keys are to be checked at the end of each working day and housed, when not in use, in approved containers or approved key boxes.

g. The keys are not to be accessible to persons who do not have authorised access to the material or to the room which the lock protects.

h. Security keys are not to be removed from an establishment without the specific authority of the EsyO.

i. In-use security keys are to attract the same protective marking as the most sensitive material that they protect and are to be stored, protected and handled accordingly.

Spare Keys

051225. The following conditions apply to spare keys:

a. Spare keys to security locks are to be held centrally, in approved security containers, by the EsyO, or a designated member of staff.

b. They are not to be held in the same container as the working key.

c. The spare keys are only to be issued to persons with authorised access to the material the lock protects, on receipt of documentation proving that the working key has been mislaid or lost. The keys are only to be issued to allow for the contents of the container/secure room to be removed and placed in appropriate secure conditions. The container/secure room is then not to be used to house protectively marked material until such time as the locks have been changed or all the keys have been located and compromise is not suspected.

d. Details of the issue of spare keys are to be recorded and the security staff informed, if the keys have been issued at 'branch' level.

e. Additional keys are only to be supplied on the written authority of the establishment security staff.

f. A record is to be kept by the establishment security staff of the number of keys issued, to facilitate control and mustering.

g. Each set of keys is to be held, either, on a special to type keyboard within an appropriate security container or be sealed in a separate envelope, marked on the outside with the following information:

(1) The key numbers.

(2) Brief details of the related security container and location.

(3) The names of the persons authorised to have access to the spare keys.

It is best practice, but not mandatory, for the envelope to be protectively marked to the same level as the highest protective marking of the material held in the container itself. The user of the container is to sign across the flap and add the date after the

envelope is sealed. The signature and flap are then to be over-sealed with clear cellulose tape of at least 19mm width.

Note: Each key issued with a lock is to be used in rotation as the in-use key for a maximum period of 6 months.

Mustering

051226. In addition to the requirement for a 6 monthly muster of all security keys on an establishment, security keys in regular use are to be mustered daily at close of work.

Identification

051227. Keys are to be labelled to facilitate their daily issue and muster. The labelling is to be such that it does not readily identify the container to which the key belongs. Key rings are to be checked frequently to ensure that keys cannot become detached.

Transmission

051228. Keys are to be transferred by hand of one authorised person to another, but where this is not possible, they are to be transmitted under safeguards appropriate to the highest protected marking to which the relevant lock gives access.

Key Security in Offices

051229. Whenever a room or building is left unoccupied, keys are to be secured. They are never to be put into furniture that does not conform with the security standards laid down within the minimum baseline measures matrix.

Promulgation of Security Key Procedures

051230. The procedure for all aspects of the handling of security keys and combinations is to be promulgated by heads of establishment in establishment standing orders.

Security Containers Returned to Store

051231. Whenever a security container is issued from or returned to store, all keys are to be tried in the lock. Keys are not to accompany the container; they are to transmitted under separate cover.

Security Containers not in Use

051232. All security keys for containers not in use are to be withdrawn and taken on charge by the ESyO. The security containers are to be locked shut pending issue of the container and key to another person.

Local Replacement or Manufacture

051233. Security keys are not to be manufactured under local establishment arrangements e.g. to replace a lost key or to create a new one.

Issue of Duplicate Keys

051234. In the event of a security key being lost or mislaid, the container must be assumed to be compromised and the duplicate key must not be used.

Ordering of Security Locks through Sub-contractors

051235. When it is necessary to order approved security locks through sub-contractors, the individual ordering the lock is to ensure that the sub-contractors annotate the order form to indicate that the lock and keys are to be sent direct to the ESyO.

Change of Appointment

051236. On change of appointment, key custodians who signed for the keys are to return them to the ESyO who will then issue them to the new custodian.

Other keys

051237. The locks and keys to non security containers or to intruder detection panels etc are not in themselves security keys but they are used to secure items and equipment in need of protection. Such keys are to be held and treated in a manner appropriate to the material they protect.

Action in the Event of Suspected Compromise or Loss of Security Key or Combination Setting

Immediate Action

051238. The following action is to be taken in addition to any other disciplinary action required under the provisions of QRs:

a. The loss or suspected compromise of a security key is to be reported immediately to the ESyO who is to inform the head of establishment without delay.

b. When the circumstances are suspicious the relevant security unit is to be requested to investigate following consultation with the PASyA.

c. As further handling may destroy evidence, the container is to be preserved for examination by the investigator.

d. Whenever there is reason to suspect compromise of any or all of the contents, immediate action is to be taken under the provision of Chapter 4.

e. DDef Sy is to be informed, by the PSyA, where appropriate in accordance with the policy at Chapter 2.

Liability for Cost of Replacement

051239. The person held responsible for the loss of a security key may be liable for the cost of the replacement of the lock.

SECTION XIII TO CHAPTER 5

MECHANICAL DOCUMENT TRANSFER SYSTEMS & AUTOMATED DOCUMENT ACCOUNT SYSTEMS

Mechanical Document Transfer (MDT) Systems

Introduction

Description of MDT Systems

051301. Mechanical document transfer (MDT) systems include those employing rails, tracks or pneumatic tubes for the carriage of documents within buildings.

Further Information, Advice and Guidance

051302. Guidance on the design and procurement of MDT systems is available from D Def Sy through PSyA staff. Authority to install a MDT system is to be sought from PSyA staff prior to detailed planning taking place at an establishment.

General Security Measures

Assessment

051303. Before the installation of a MDT is considered an assessment is to be made of the security implications in running the system or during installation, maintenance or repair. The cost-effectiveness of installation must also be justified.

Preventing Unauthorised Access

051304. The security concerns are to be concentrated on ensuring that unauthorised persons do not gain access to any protectively marked material which it is being carried by a MDT. Access is to be denied to:

a. The document carriers.

b. The tubes, tracks or rails, especially those running between buildings or through isolated or infrequently used parts of buildings.

c. The electric power or compressed air supplies for the system.

d. The system control panel (some systems have their controls on the carrier).Detailed Security Measures

Level of Physical Security Protection

051305. The level of physical security protection required will depend on:

a. The threat.

b. The level of protectively marked material carried.

c. Whether or not the system is used exclusively within a secure area.

Covers and Lids

051306. Covers or lids on carriers may need to be designed so that they can be locked during transit and when they arrive at a destination where authorised staff may be temporarily absent. This may not be necessary if the system is routed exclusively through a secure area.

Design of Hinges on Lids

051307. The hinges on the lids of carriers are to be designed so as to prevent their removal when the lid is closed and locked.

Ventilation

051308. Where motor ventilation is necessary care is to be taken to ensure that this does not allow access to the documents being carried.

Ducting

Design of Ducting

051309. Ducting through which the MDT runs is to be designed so that it is not possible to halt or remove carriers while they are in transit. Access to control panels which, on some systems, are situated on the outside of the carrier, is to be denied as these control the route and destination of the carrier.

Location of Ducting

051310. Ducting may be run between buildings providing the buildings are within a secure perimeter and any maintenance access panels are designed so as to prevent unauthorised access to the track and the carriers.

Unauthorised Entry to Building

051311. The ducting is not to be capable of providing a means of unauthorised entry to the building or secure area during silent hours or when the MDT system is not in operation.

Security

Supervision

051312. Arrangements are to be made to ensure that terminals are properly supervised and given suitable protection when left unattended.

Security of Carriers

051313. Where carriers containing protectively marked documents are held at terminals outside working hours the following is to be ensured:

a. The carriers and contents are to be secured to an appropriate standard.

b. Precautions are to be taken to ensure that no carrier is left between terminals or routed to an unmanned or unprotected terminal.

c. The control system is to be designed to indicate, at the central control panel, whether any carriers are still in transit.

Protection of Despatch Control Unit

051314. Where there is a central despatch control unit it is to have protection during silent hours, it is not within a secure area, either by securing the room or by installing intruder detection devices.

Emergency power

051315. Provision is to be made for a standby power supply.

Transmission between Secure Zones

051316. When MDT systems are used for the transmission of protectively marked documents between two secure zones in an otherwise insecure building, the normal rules for enveloping and receipting should apply (see Chapter 4; Transmission of Protected Assets). However, in systems working solely between two areas where all operating personnel at both terminals are authorised to see the material and where the tube or track between the terminals has adequate physical protection, protectively marked documents may be transmitted un-enveloped in unlocked carriers.

Automated Document Accounting Systems (ADAS)

Introduction

051317. Automated systems may be used in place of manual systems to account for protectively marked documents.

Further Information, Advice and Guidance

051318. Guidance on the design and procurement of ADAS systems is available from D Def Sy through PSyA staff. Authority to install an ADAS system is to be sought from PSyA staff prior to detailed planning taking place at an establishment.

Efficiency

051319. Where an ADAS is part of a larger electronic office project, it has the potential to improve efficiency. Although there may be little saving in staff time spent on the initial registration of documents, an ADAS has the potential to reduce the time devoted to the subsequent movement of paper where they pass regularly between different locations.

Facilities

051320. An ADAS which is intended to replace manual accounting of protectively marked documents must be capable of:

a. Recording and where necessary creating a receipt (with appropriate details) of each document or file.

b. Registering the location of each document or file.

c. Recording the temporary and the final disposal of each document or file, eg. document to file, despatch, destruction etc.

d. Produce a list of each entry on the system to facilitate audit trails, routing lists, file lists etc.

e. Providing a regular back-up of the system.

Security Measures

Access to the ADAS System

051321. Access to the ADAS system is to be limited to those authorised to use it and the establishment security staff; the following software security measures are to be applied:

a. No data deletions are to be permitted; however, a facility is to be included to annotate incorrect entries.

b. All data alterations are to be recorded after initial data entry and verification.

Additional Security Measures

051322. In certain circumstances, security measures in excess of those detailed above may be required. Factors affecting the extent of additional security measures include:

a. The level of protection required by documents controlled by the ADAS.

b. The number and location of terminals.

c. The physical protection afforded by the environment within the establishment.

d. The requirement for 'need-to-know' separation.

SECTION XIV TO CHAPTER 5

ACCOMMODATION MOVES

General

Introduction

051401. This Section gives information about accommodation moves involving protectively marked assets. To ensure that a move is successful, it is essential that adequate planning of the security aspects of the move is undertaken at an early stage. All personnel involved are to be made aware of their responsibilities.

Further Information, Advice and Guidance

051402. Further advice on any aspect of a move may be obtained from Command security staff.

Planning

Involvement of Security Officers

051403. The ESyO and/or other sub-unit security officer is to be involved in the security planning of the move at the commencement of arrangements being formulated. They are to be fully aware of and contribute to the plans of senior management.

Responsibilities of Security Officers

051404. The ESyO and other sub-unit security officers involved have the following responsibilities:

a. To obtain structural plans of the new accommodation, and become familiar with any inherent problems that may require action, if possible before the move is undertaken.

b. Check the effectiveness of any security measures that may already exist in the new accommodation.

c. Ensure that the allocation of accommodation takes full account of any requirement for secure zones or registries and secure communications, and that whenever possible SECRET and TOP SECRET material is located away from the ground floor (see Section II of this Chapter).

d. Identify occupants of adjacent buildings especially when considering the possibility of overlooking, overhearing and the TEMPEST threat.

e. Ensure that funding is allocated for any alterations, or additional security measures that may be necessary.

f. Monitor proposals for any structural alterations, and check that they do not adversely affect security.

g. Establish a close liaison with other personnel with security responsibilities where the accommodation is shared with another establishment and agree on security responsibilities.

The Move

Actions to be Taken

051405. In planning the move it is necessary to consider the distance involved and the amount of protectively marked assets to be moved. All moves of protectively marked assets are to be in accordance with a movement plan agreed in advance by the ESyO. Personnel are to be made aware of their responsibilities during the move. All stages of the move are to be supervised by security staff or appropriately cleared personnel who are to be fully briefed on the details of the move plan. In addition the following is to be actioned:

a. **At all stages of the move.** Adequate security is to be provided for the protectively marked assets at all stages of the move. This includes at the vacated premises, in transit and at the new accommodation.

b. **Transit crates.** Protectively marked assets are not to be transported in security containers. Unless the amount of such material is small, approved transit crates are to be used; The following rules apply to transit crates:

(1) Transit crates that can be effectively sealed are to be filled by those responsible for the protectively marked assets.

(2) The lid is to be secured and sealed using only recommended seals.

(3) Those crates that need to be protected are to be identified, and their destination in the new building clearly marked.

(4) Crates are to contain packing lists to facilitate subsequent checking.

(5) Labels on crates are not to indicate the protective marking of the contents.

(6) Crates are to be redistributed in accordance with staff location requirements; seals are to checked and the contents transferred into approved security containers.

(7) On completion of unpacking, all crates are to be checked to ensure that they have been emptied of their contents.

(8) An appropriately vetted escort is to accompany crates containing material protectively marked SECRET and above.

c. **Commercial companies.** The use of commercial companies to transport protectively marked assets is acceptable; however, a security escort, is to remain with the vehicle whenever it contains material bearing a protective marking and/or a descriptor.

d. **Additional movement actions.** The following additional actions apply:

(1) It may be advisable to inform the police of the route of the move, particularly if a number of vehicles are involved.

(2) Times of moves are to take account of likely traffic conditions.

(3) Contingency plans are to be prepared to cover accidents, breakdowns or diversion of load or other emergencies.

e. **Security containers.** The following actions in respect of security containers are to be carried out:

(1) Security containers are to be transported with their shelves stacked securely at the bottom of the container.

(3) The doors are to be locked.

(3) Combination locks are to be set to manufacturers' settings and locked.

(4) The keys for key-locked security containers are to be carried separately under secure arrangements.

f. **Accommodation checks.** Thorough checks under the control of the ESyO are to be made of the vacated accommodation to ensure that nothing has been left behind. Where premises are to be handed over to Defence Land Agents, the ESyO is to seek the advice of the appropriate PSyA and request the help of the appropriate Security Unit.

g. **Overseas moves.** When material is to be moved overseas, PSyAs are to be consulted.

Closure of Establishments

051406. Establishments are to seek the advice of their PSyA/security unit in the event of the establishment being scheduled for closure and the estate being sold. In particular, the following criteria are to be considered:

a. Plans are to be made for the disposal of security installations such as the AC12 IDS. The cabinets for AC12 are to be removed from the walls and returned to SSG. Documents and drawings for the facility are to be destroyed or otherwise securely disposed of.

b. Logs/records for access control systems are to be destroyed or otherwise securely disposed of.

c. Security or operational fittings and fixtures that could compromise the mode of operation of other establishments if disclosed should be removed.

SECTION XV TO CHAPTER 5

REPROGRAPHIC MACHINES

General

Definition

051501. The term reprographic machine is defined as any type of machine capable, by any process, of producing copies of a document (eg photocopiers, facsimile machines, joint fax/photocopiers, laser printers, etc).

Further Information, Advice and Guidance

051502. The following information, advice and guidance on reprographic machines can be obtained:

a. Advice on the suitability of all types of reprographic machinery - including new technologies - for use with protectively marked material can be obtained from D Def Sy via appropriate PSyA staffs.

b. Advice on problems arising from the application of the policy contained in this Chapter is to obtained from PSyA staffs.

c. Advice on machines with AACS (restrictive use system) can be obtained from D Def Sy or the Catalogue of Security Equipment (CSE).

Control of Use

Control of Access

051503. Access to reprographic machines is to be strictly controlled to prevent unauthorised copying of protectively marked material.

Methods of Control

051504. Where the risk of unauthorized disclosure is high, or when SECRET and TOP SECRET material is involved, the following methods of control apply:

a. **Dedicated personnel.** Whenever possible, only dedicated personnel are to be authorised to carry out copying. Alternatively, personnel are to seek permission to use the machine on each occasion.

b. **Use of AACS.** The use of an AACS (restrictive use system) is to be encouraged; many photocopiers have an integral system of control, or alternatively, 'add-on' machines are available. It is MOD policy that all AACS are to incorporate Watermark^{R} technology. Where selecting an 'add-on' system, those which combine a card with personal identification number (PIN) offer the greatest level of security. Most systems (should it be required) have the facility to provide a print out of details such as the number

of copies made against a PIN or entry code, together with time and date. Such systems control who has had access only, and not what has been copied.

c. **Switch box cover.** When not in use, power supplies are to be protected by an approved switch cover (Order Code 24.55.0015 - 13 amp or 24.55.0022 - 30 amp as appropriate) which is secured by an approved padlock.

d. **Removal of key counter.** Where so fitted, the detachable 'key counter' on photocopiers is to be removed and stored securely.

e. **Siting.** Wherever possible, machines are to be sited:

(1) In a locked room.

(2) Away from windows so that reproduction cannot be overlooked.

f. **Use of F102.** The reproduction of SECRET and TOP SECRET information (including drafts) is to be recorded in MOD F102 which are to be administered in accordance with the instructions in Chapter 4.

Potential Risks

051505. Reprographic machines can suffer faults or be vulnerable to attack in the following ways:

a. Operators of reprographic machines may fail to clear the machine of original and copy material after use.

b. Copies may become trapped in the machine, only being revealed during servicing. In the event of a machine malfunction, users are to ensure that any trapped copies are identified and removed for secure disposal.

c. Parts of certain machines such as memory chips, drums, belts and cartridges, may retain images of previous copies.

Maintenance and Disposal

051506. The following procedures apply for maintenance and disposal of reprographic machines:

a. Machines are to be thoroughly examined for trapped copies prior to servicing or maintenance.

b. Where possible all such work is to be supervised.

c. In particularly sensitive areas, special arrangements to prevent compromise of information are to be made.

d. **Photo receptor belts and drums.** Photo receptor belts and drums may contain protectively marked information. If it becomes necessary to dispose of the machine or to have the belt/drum removed for repair the maintenance engineer should not be allowed to remove them from the establishment until the measures detailed below are followed:

(1) If it is possible to operate the machine, the lid of the photocopier should be closed and five blank copies produced. This procedure will clean the drum or belt of any images that may be retained and any markings on the paper will cease to appear.

(2) When it is not possible to operate the machine, the belt/drum should be removed from the machine by the maintenance engineer and wiped clean with a suitable non-abrasive cleaning material such as Isopropyl Alcohol. This procedure is only required if the last copying procedure contained information protectively marked CONFIDENTIAL or above, or in the event that the protective marking of the last procedure could not be established.

e. **Digital reprographic machines.** In the case of reprographic machines that have a memory facility, it should be established whether the memory is volatile or non-volatile;

(1) A machine that has a volatile memory can have the memory erased simply by switching off the power supply.

(2) If the memory is non-volatile it is possible to overwrite any protectively marked information by running 5 non-protectively marked documents through immediately afterwards. When it is not possible to operate the machine, advice should be sought from the Sector Security Authority regarding safeguarding any protectively marked information that may be retained in the memory.

Power Supply

051507. The machine should be permanently connected to the building electrical power supply via a non-detachable power supply cord, protected by a control box. Both 1 phase and 3 phase photocopiers may be hardwired however, to satisfy Health and Safety Legislation (EN 60950), they are to be hardwired into an isolator and it must be possible to lock off or remove the in-line fuses to the isolator. Where permanent connection is not possible, the machine must be able to be isolated from the power supply by a locking device such as a security plug box (Catalogue of Security Equipment - 24.55.0039) or an AACS. At ceasework, keys are to be stored in a security container.

Tempest

051508. Establishments intending to install electronic reprographic machinery in areas requiring TEMPEST consideration are to obtain advice from PSyA staffs.

This page intentionally left blank.

SECTION XVI TO CHAPTER 5

DESTRUCTION OF PROTECTIVELY MARKED WASTE

General

Introduction

051601. Care is to be taken of all protectively marked waste material until it has been thoroughly destroyed in accordance with the regulations set out below.

Further Information, Advice and Guidance

051602. The following further information, advice and guidance can be obtained:

a. Details of all SEAP approved destruction equipment and destruction facilities are contained in the Catalogue of Security Equipment (CSE).

b. Establishments are to contact their Command security staff for details of the equipment and facilities.

General Principles

051603. The following general principles apply:

a. **Protection.** Pending destruction by an approved method, protectively marked waste retains its sensitivity, and is to be given the appropriate protection.

b. **Separation.** Protectively marked waste, before destruction, is to be clearly identified and kept separate from other waste.

c. **Authorised access.** Personnel not authorised to have access to protectively marked material are not to be allowed direct access to waste that is so marked. At units overseas, all protectively marked waste is to be destroyed by UK personnel who are cleared to the appropriate level of access.

d. **Accumulation.** No unnecessary accumulation of waste is to occur.

Administrative Procedures

051604. The administrative procedures detailing the rank of personnel able to undertake the destruction and associated documentary requirements are contained in Chapter 4.

Rules for Destruction

051605. Destruction of protectively marked waste is to follow the rules below:

a. **RESTRICTED**. RESTRICTED waste is to be destroyed by a method approved for each particular waste type (see Annex A). There is no requirement to use SEAP approved equipment. The rules for RESTRICTED waste are as follows:

(1) Small quantities of paper waste may be disposed of as unclassified waste, eg in waste paper bins, provided it is torn into small pieces and mixed with other unprotected paper waste prior to disposal.

(2) Waste may be sent to, or collected by, an approved commercial company that has been contracted for this purpose. Approval for the use of a commercial contractor is to be obtained by establishments from Command security staffs.

b. **CONFIDENTIAL, SECRET and TOP SECRET.** Waste marked CONFIDENTIAL and above is to be destroyed by a method approved for each particular waste type (see Annex A), using SEAP approved equipment or methods. The principal methods of destruction are:

(1) Incineration.

(2) Disintegration.

(3) Hammer-milling.

(4) Shredding.

(5) Pulping.

(6) Acid and chemical techniques.

c. **Certification.** The destruction of TOP SECRET and SECRET material is to be witnessed and certified by two suitable vetted persons, one of whom must be an officer not below the rank of Warrant Officer (or a Senior NCO nominated by the Commanding Officer), Administrative Officer or equivalent. The destruction of material marked CONFIDENTIAL, where recorded in a MOD F 102, may be undertaken by one authorised member of the Armed forces or Civil Service.

The methods are described in more detail below. In addition to destroying waste on site, approved destruction facilities can be used to destroy all waste types.

Collection, Handling and Storage of Waste

Handling prior to Destruction

051606. The following rules are to be observed for the handling of protectively marked material prior to its destruction:

a. The waste is to be held in an appropriate container according to its protective marking.

b. General rubbish such as cans, bottles, food and broken glass is not to be included with protectively marked waste.

c. The waste sacks, when filled, are to be secured before being taken to the central destruction or collection point by appropriately cleared personnel.

d. Personnel not authorised to have access to protectively marked material may be employed as messengers provided they are supervised by a suitably cleared person.

e. Bags of protectively marked waste, awaiting bulk destruction, should be sealed in such a way that tampering will be immediately apparent.

Waste Sacks

051607. Waste sacks for the collection of protectively marked waste are to be sufficiently strong (Eg. double-lined) to withstand rigorous handling. Where required, special Kraft paper sacks identified by HMSO code numbers are available as follows:

a. Code 971-003 multiwall printed in red for burning.

b. Code 971-004 multiwall printed in black for pulping.

Records

051608. The following recording action in a permanent notebook is to be taken with respect to sacks of protectively marked waste:

a. A record of the number of sacks collected is to be kept by those responsible for safeguarding protectively marked waste (e.g. registry staff).

b. When the sacks are stored pending destruction, a record is to be kept of the number received into store, and of the number subsequently destroyed or handed over to, or sent for destruction by a commercial company.

c. When handing sacks to a commercial company, receipts are to be obtained.

d. The records of sacks received, stored and destroyed is to be checked regularly by establishment security officers.

Methods of Destruction

Incineration

051609. Incineration is the most effective method of destroying large quantities of most types of protectively marked material. Criteria for the equipment is to be as follows; it is to:

a. Be lockable so that, once loaded, the waste cannot be removed by unauthorized personnel.

b. Have a trap to prevent readable pieces of material being carried up the flue.

c. Incinerate to a fine ash residue, which is capable of being sifted to ensure that the destruction process is complete.

d. Be so designed that, if there are moving parts such as chain grates, the material being incinerated cannot escape from the combustion chamber.

e. Comply with existing environmental legislation and the manufacturers' operating instructions. It is to be maintained correctly, and the manufacturer is to be consulted in the event of any operating difficulties.

051610. *Spare.*

The Destruction of Paper and Paper-based Waste

Shredding

Baseline Measures for Shredding Protectively Marked Material

051611. Protectively marked paper, carbon paper, card, and tape is to be shredded in accordance with the following baseline measures before it may be treated as non-protectively marked waste:

a. Material marked RESTRICTED may be destroyed on any shredder.

b. Material marked CONFIDENTIAL or above is to be shredded using equipment which ensures that no more than two adjacent characters are legible in the shred size. The waste must:

(1) Be cross-cut shredded.

(2) Be shredded to a size of no greater than 60 sq mm.

(3) Have a shred width not exceeding 4mm.

c. Papers are to be inserted as whole pages into the shredder with the lines of print at right angles to the direction of shredding.

Additional Measures

051612. The following additional measures are to implemented:

a. **Examination of shreddings.** Shreddings are to be examined periodically by establishment security staff to ensure that the maximum permissible shred size specification is not being exceeded.

b. **Maintenance and servicing of equipment.** Before maintenance work or servicing is undertaken on a shredding machine, it is to be examined to ensure that it does not contain any un-shredded or partially shredded material.

c. **COMSEC and codeword.** The standards to be achieved for COMSEC and codeword material are:

(1) With the exception of paper tapes, paper is to be crosscut, with the lines of print at right angles to the direction of shredding.

(2) The maximum shred width is to be 1 mm and length of crosscut 20mm.

(3) The shreddings are to be the product of 12 or more A4 size sheets (or equivalent) of the same colour and thickness. The shreddings of codeword and COMSEC material can be mixed with shredded material originally of another protective marking.

Pulping

051613. Pulping machines are effective in destroying most paper and card and, with certain provisos, waterproof and wet strength paper, flat photographic film and laminates. Pulping is not to be used for the destruction of plastic materials, lithoplates, paper tapes or films in rolls.

Disintegrators & Hammer-mills

051614. Hammer-mills and disintegrators can be used for the destruction of protectively marked paper and paper based materials.

Baseline Measure - CONFIDENTIAL or Above

051615. A grille size of no larger than 6mm is to be used when destroying waste marked CONFIDENTIAL or above.

RESTRICTED Waste

051616. Waste marked RESTRICTED may be destroyed using any grille size.

The Destruction of Magnetic Media

Definition

051617. The term magnetic media is used to cover all forms of electronic, audio and some types of optical media such as hard and floppy disks, microchips and audio tapes, etc.

Incineration

051618. All forms of magnetic media may be destroyed by incineration (see para 051609). Due to the toxic nature of certain substances used in some forms of magnetic media, current regulations regarding the disposal of waste are to be complied with.

Disintegrators

051619. Disintegrators and hammer mills can be used for the destruction of all forms of magnetic media.

Baseline Measure

051620. When destroying waste marked CONFIDENTIAL or above, a grille size of no larger than 6mm is to be used.

RESTRICTED Waste

051621. Waste marked RESTRICTED can be destroyed using any grille size.

Use of Pre-breaker

0516182. Printed circuit boards (PCBs) and microchips can damage the blades of disintegrators. When destroying large quantities of these materials a pre-breaker is to be used. Hammer-mills are specifically designed to deal with such materials.

Noise Levels

051623. Disintegrators and hammer-mills are noisy in operation and are not suitable for use in offices or quiet locations.

Sanding

051624. When the quantities of hard disks to be destroyed are small, the magnetic media bearing surface of the disks may be removed by emery paper, a disc sander or emery wheel. The remaining metal platter is then to be disposed of as non-protectively marked waste. Appropriate Health and Safety precautions must be applied when using this method.

Shredding

051625. Floppy disks can be destroyed using approved shredders, providing the rules described in paras 051611 and 051612 are followed. Due to the high density of

information contained on floppy disks, it may be possible to retrieve information from surviving fragments. Care is to be taken when disposing of shredded disks.

Acid and Chemical Techniques

051626. Acid and chemical techniques may be used to destroy all levels of protectively marked magnetic media. Details of approved commercial facilities are listed in CSE. Establishments are to obtain details from Command security staff.

The Destruction of Microform

General

051627. Protectively marked microform i.e. microfiche and microfilm, is to be destroyed by equipment, processes or facilities approved by SEAP. Microform contains a very high density of protectively marked information. The approved methods detailed below are divided into those which provide total destruction, and those where it may be possible to retrieve information from surviving fragments, that is partial destruction. However, the threat to such waste in the UK is considered to be very low and these methods may be used by establishments in the UK providing microform is destroyed using approved equipment. Details of approved equipment can be obtained from the CSE held by Command security staff.

Total Destruction

Incineration

051628. Microform is to be incinerated as follows:

a. Fed into the incinerator whole, i.e. not cut, shredded or disintegrated beforehand.

b. Strictly accounted for right up to the point where the ash or dust has been examined for total destruction.

Microform Destructor

051629. Microform may be destroyed using a SEAP approved microform destructor.

Commercial Services

051630. Details of commercial destruction services approved to destroy protectively marked microform can be found in the CSE, obtained via Command security staff.

Partial Destruction

Shredding

051631. Microform destroyed using this method is to conform to the following rules:

a. Be destroyed using SEAP approved microform shredders.

b. The manufacturer's operating instructions are to be followed.

c. The residual waste is to be thoroughly examined.

d. The waste is to be disposed of in such a way as to minimize the chance of retrieval.

Disintegrators and Hammer Mills

051632. Microform may be destroyed using SEAP approved hammer mills and disintegrators, using a screen size no greater than 2mm. The microform is to be mixed with paper when fed into the disintegrator or hammer-mill.

Emergency Destruction

Overseas Theatres

051633. The need for emergency destruction of protectively marked material should only arise in operational theatres overseas (see also Chapter 14 on Operational Security). The following precautions are to be taken:

a. The quantity of SECRET and TOP SECRET material held is to be kept to a minimum.

b. An order of priorities detailed in the form of written instructions for destruction is to be established and kept in a location known to personnel, to which access can be obtained without delay in an emergency, eg on the back of a strong room door.

c. A plan is to be prepared for using all the available destruction equipment. Periodic checks are to be made to see that the equipment is serviceable and that staff know where it is and how to operate it.

d. An officer is to be appointed IC emergency destruction.

UK Establishments

051634. HOEs are to ensure that simple emergency plans are in existence which stipulating the following:

a. Which categories of document are to be destroyed.

b. The persons responsible for destruction.

c. The precise action required.

d. Destruction priorities.

The plans are to be checked and reviewed at regular intervals. The emergency destruction plan is to be built into establishment operational emergency plans. Emergency exercises should include destruction drill exercises.

Emergency Destruction on Ships

051635. In addition to the instructions in this part, ships are to comply with the extra regulations at Annex B.

Emergency Destruction in Aircraft

051636. There will be little time in an aircraft emergency in which to destroy protectively marked material. However, if possible, an attempt is to be made to prevent material falling into the hands of hostile forces. Where possible, documents are to be torn into pieces as completely as possible and dispersed. Where possible, protected equipment should be smashed beyond use and dispersed as widely as possible.

Methods of Emergency Destruction

Approved Equipment

051637. Full details of approved emergency destruction equipment are to be found in the CSE.

Emergency Destruction on Military Operations Overseas

051638. Instructions for emergency destruction on military operations overseas will be promulgated by the relevant operational HQ at the time of deployment; Chapter 14 gives further advice in this area. Sodium nitrate emergency destruction kits (EDK) can be obtained through supply sources on the authority of Command security staff for the destruction of TOP SECRET documents overseas, which because of their nature cannot be destroyed in advance. The kits are classified as explosive items and must be handled accordingly.

Other Emergency Methods

051639. It is not possible to lay down standard methods of emergency destruction since these will depend on the prevailing conditions; Headquarters may possess shredding machines, whereas other establishments may have to rely on open fires. In general, the method used is to be as simple as possible and plans are to recognise what is likely to be available in emergency circumstances. For example an establishment which uses only diesel fuel will have to have a 'starter' for igniting the fuel (such as detonators) or arrange to carry a special supply of petrol if this cannot be done.

Planning Points

051640. Further points to consider are as follows:

a. Since fires will not burn without oxygen, the brazier or other container must have enough holes in it to allow sufficient air to enter.

b. Where possible, a wire cage is to surround the incinerator to prevent loose pages being carried away by the wind or thermal up-draught.

c. The mass of ash should be constantly stirred and lifted with a long poker to ensure that no pages are left and that the ash is broken up.

ANNEX A TO SECTION XVI

TO CHAPTER 5

METHODS OF DESTRUCTION

Material	Preparation	Incineration	Shredding	Pulping	Disintegration	Hammer Milling	Notes
Paper	Remove paper clips when pulping or shredding	Yes	Yes	Yes	Yes	Yes	
Carbon Paper	Remove paper clips when pulping or shredding	Yes (a)	Yes	Yes (b)	Yes	Yes	(a) Mix with paper. (b) Potential of discolour-ing, if mixed with paper.
Punched paper tape and cards	Remove paper clips when pulping or shredding	Yes	Yes	Yes	Yes	Yes	
Film (unmount-ed)	None	Yes	Yes	Yes	Yes	Yes	Mix with paraffin to assist pulping.
Film (Reels)	Remove from reel before shredding	Yes	Yes	Yes	Yes	Yes	
Film (Plate or mounted)	None	Yes	No	No	Yes	Yes	
Microform	None	Yes	Yes (a)	No	Yes	Yes	(a) Mix with paper.
Litho printing plates	Break into small pieces	Yes	No	No	Yes	Yes	

Material	Preparation	Incineration	Shredding	Pulping	Disintegration	Hammer Milling	Notes
Printed circuit boards	None	Yes	No	No	Yes	Yes	
Magnetic core stores	Break into small pieces	Yes	No	No	Yes	Yes	
Magnetic Disks	Dismantle & break into small pieces	Yes	No	No	Yes	Yes	See JSP440, Vol 3, Chapters 4 & 5.
Magnetic tape (digital)	Radial saw cut before incineration	Yes	No	No	Yes	Yes	
Magnetic tape voice & video (analogue)	Radial saw before incineration	Yes	No	No	Yes	Yes	
Floppy discs	None	Yes	Yes (a)	No	Yes	Yes	(a) Mix with paper.
Printer ribbons	None	Yes	No	No	Yes	Yes	When using hammer mills, mix with paper.
Plastic materials	None	Yes	No	No	Yes	No	

ANNEX B TO SECTION XVI

EMERGENCY DESTRUCTION OF PROTECTIVELY MARKED MATERIAL IN SHIPS

Introduction

1. **Section XVI to Chapter 5.** This Annex is to be read in conjunction with Section XVI, Chapter 5.

2. **Contingency plan.** Commanding Officers are to have a contingency plan for the rapid destruction of all TOP SECRET, SECRET and CONFIDENTIAL information and material in ships in an emergency. The plan is to be ready to be put into operation at any time should hostilities break out or there is another necessity for it to arise.

3. **Quick and effective destruction.** All departments within a ship are to plan for the quick and effective destruction of their protected information and material.

4. **Pre-positioning of equipment.** Equipment required for the destruction of the information or material is to be pre-positioned and on-hand should the need arise.

5. **Training exercises.** Training exercises are to be conducted regularly to ensure that all personnel know how to carry out their tasks in an emergency.

Operations in High Threat Environments

6. **Staff planning.** The CINC may direct that ships having to operate in a high threat environment (HTE) are to carry a reduced set of documents. The senior officer ordering an operation or movement involving ships in a HTE is to include orders to the ship concerned to comply with these instructions by landing their surplus documents before sailing or, if already at sea, by destroying their surplus documents.

7. **Planning prior to sailing.** When ships are about to sail into a HTE in shallow waters, the commanding officer is to action the following:

   a. Arrange that only those documents that are essential to the operation are carried.

   b. TOP SECRET documents necessary for the operation are to be bagged and weighted before the start of the operation.

c. All other protectively marked documents are to be landed before sailing and placed in the custody of a UK diplomatic or military official.

d. The documents are to be securely stowed in security chests or sealed bags to be moved ashore when the occasion arises; receipts are to be obtained for them. The name of the ship is to be clearly marked on the outside of the chests or bags.

8. **Action if at sea.** Where the ship is already at sea when ordered to enter a HTE, the following applies:

a. Orders may be given by the relevant command authority for all protectively marked documents and material not essential for the operation, to be destroyed.

b. Destruction is to be by shredding or burning, or throwing overboard in weighted and eyeletted sacks where no facilities exist.

c. Where no orders have been received for the disposal of surplus documents, the Commanding Officer may order the action detailed at para 8a where he believes it is necessary; He is to report the action taken to the necessary authorities at the earliest opportunity.

d. Instructions for the disposal of superseded crypto and communications publications are to be rigidly enforced.

e. Officers are to use their discretion in ordering the destruction of protectively marked documents in an emergency, and no risk is to be taken of any of them falling into the hands of a hostile force.

Emergency Destruction in Ships

9. **Priorities for destruction.** Documents and equipment are to be destroyed in order of priority as assessed by the head of department.

10. **Priorities.** Priorities for destruction include the following:

a. Keying material.

b. Cypher tables.

c. Machine settings.

d. Superseded crypto.

e. TOP SECRET documents.

f. Cryptographic material not needed for encrypted communications during danger periods.

g. The scrambler box mechanism of cryptographic machines.

After the destruction of other protectively marked information, where time permits, inserts, permits, rotors machines, drums and adaptors are to be destroyed by hammer or other suitable tool. Wiring is to be torn out and the separate parts thrown overboard in different directions.

11. **Use of security containers.** All protectively marked documents that are operationally essential are to be stored in appropriate containers. In the event of the ship sinking. These documents are to be left in position to go down with the ship.

Emergency Destruction Reports

12. The following applies to the reporting of emergency destruction:

a. When documents are lost or destroyed under emergency conditions, every effort is to be made to report the fact and the manner of disposal of the documents.

b. An initial report (i.e. by signal) is to be sent to the relevant command authority giving sufficient detail to allow a decision to be made whether the documents have been compromised.

c. A full written report is to be forwarded by the Commanding Officer or senior surviving officer, to the relevant command authority detailing how all the protectively marked material was disposed of.

Action in the Event of an Emergency

13. Should an emergency arise, such as a collision at sea, sinking or fire, action is to be taken to safeguard protectively marked material; where there is a necessity for emergency destruction procedures to be initiated due to the ship being in a HTE, the directives on emergency destruction contained within this Annex are to apply.

This page intentionally left blank.

SECTION XVII TO CHAPTER 5

CONFERENCE SECURITY

General

Aims

051701. The aims of conference security are as follows:

a. To prevent unauthorised access to protectively marked information.

b. To protect persons from violence and intimidation.

c. To protect property from damage.

Further Information, Advice and Guidance

051702. The following information, advice and guidance on conference security can be obtained:

a. Further advice on the security procedures required for conferences either on Defence establishments, or where they are held in commercial premises, can be obtained from appropriate PSyA staffs or from the Services' specialist security units: the Area Security Team for the Navy, the Local MI Bn unit for the Army, local P&SS unit for the RAF.

b. For information on technical and non-technical inspections, see Chapter 15.

c. For further precautions on overlooking and overhearing see Section V to this Chapter.

Conference Security Officer

Appointment of CSO

051703. A conference security officer (CSO) is to be appointed by the head of establishment. The CSO is to be responsible for all security in the conference area. Consequently, the CSO is to have a sound working knowledge of protective security. Where the CSO is not the ESyO, he/she is to briefed by the establishment security staff on the procedures to take.

Location of CSO

051704. The CSO is to be provided with an office or appropriate area near the main entrance and be provided with supporting personnel and equipment as necessary.

Security Plan

051705. The CSO is to prepare a security plan for the conference, based on an assessment of the risks involved. This is to take into account:

a. The nature of the threats including, where appropriate, any specific to foreign personnel. Requests for threat assessments are to be made through PSyA security staff.

b. What needs to be protected - eg Classified/sensitive discussions, documents, people.

c. Whether any special security considerations apply, such as the need to conform with NATO requirements.

d. What additional protective security measures may be necessary - eg conference venue (within protected area/establishment perimeter/off establishment commercial building), technical security inspections, protection of communications equipment, provision of a separate secure zone for delegations.

e. Whether close protection of VIPs is required and what arrangements should be made beforehand with the local Service/civil police and Service security team as appropriate.

f. Guarding/reinforcements requirement.

g. The need for a contingency plan against terrorist attack, including the identification of bomb-safe areas within the building.

Access Control

051706. The CSO is responsible for arranging control of access to and within the conference building. The number of entrances to the conference building is to be kept to a minimum.

Passes

051707. The following applies with regard to passes:

a. The best practice is for access to the conference to be pass-controlled, this can be by locally produced passes that are different to any other pass in use on an establishment and that can be easily cross-checked against a master list of delegates.

b. Conference passes are to clearly indicate the dates of validity of the pass.

c. Passes are to be large enough to be easily checked by the guards and designed so that they can be worn at all times i.e. fitted with a chain or clip.

Secure Zones

051708. Where so required, the CSO is to decide which are to be secure zones i.e. those areas within the conference building to which only certain delegates, authorised officials and security staff will have unescorted access. They must be clearly defined and access to them controlled. Their number will depend on the level of protectively marked information to be discussed, the lay-out of the building and the requirements of the conference organisers.

Controlled Areas

051709. Outside the secure area but within the conference site/building there may be other areas that may need to be pass controlled.

Document Security

051710. Document security within each delegation is the responsibility of the delegation. The CSO is responsible for document security for any conference secretariat and is to make arrangements for the typing, collation and reproduction of protectively marked documents to be done in one secure area. At the end of the conference the CSO may need to make arrangements to forward protectively marked documents to delegates parent establishment using the correct channels.

Protectively marked waste

051711. The following applies with regard to protectively marked waste:

a. Where facilities are so required, the CSO is to ensure that there are adequate facilities for the collection and disposal of protectively marked waste.

b. Where necessary, an approved shredder is to be installed for use by the delegations and where required another for the secretarial staff.

c. The CSO is to ensure that the shreddings are given adequate protection.

Security Containers

051712. Where required, suitable security containers are to be provided for the storage of protectively marked material. The CSO is to make provision for key security if containers with key locks have been issued.

Tape Recorders

051713. Tape recorders are not to be taken into the conference without the prior written permission of the CSO. Tapes are to be appropriately protectively marked and accounted for.

Technical Security

051714. When highly protectively marked information is to be discussed, consideration is to be given to taking measures against eavesdropping.

Simultaneous Interpretation Equipment (SIE)

051715. SIE for use at official conferences is held by SAFE/SSG and can be requested by establishments via PSyA staffs. There are two types of SIE:

a. **Secure equipment.** For use only at conferences where the subject matter is SECRET or above.

b. **Non-secure equipment.** For use at all other conferences.

Integrity of Equipment

051716. Establishments will be required to satisfy SAFE/SSG that suitable arrangements have been made to ensure the integrity of the equipment while it is under their control.

Arrangements by CSO

051717. The CSO is to ensure the following procedures are actioned in respect of SIE:

a. No unauthorised person has access to the equipment after it has been installed.

b. The rooms in which the equipment is installed are to be locked when unoccupied and maintained to a standard agreed with SAFE/SSG.

c. There are suitable arrangements for the supervision of cleaning and maintenance.

d. The recording and transcription of any tapes during the conference will only take place in approved conditions.

e. No headphones or other equipments are removed from the conference room or interpreters' booth during the conference.

Special Features

051718. The CSO will be told by SAFE/SSG of any special features that will indicate that the equipment may have been tampered with. If tampering is suspected or there

has been unauthorised access to the equipment, PSyA security staff and SAFE/SSG are to be informed without delay.

Room Security

051719. The CSO is to implement the following:

a. That all personnel are aware of the need for proper room security.

b. Door keys are not removed from the conference building.

c. The routine silent hours patrolling requirement.

d. Doors of those rooms that have not been technically inspected are to be left open after working hours.

e. Maintenance and cleaning staff who do not hold appropriate passes are to be supervised.

Security Breaches

051720. Security breach reports are to be forwarded by the guard force to the CSO and ESyO, if different, without delay.

Security and Emergency Instructions

051721. Where required the CSO is to issue security and emergency instructions for delegations and others attending the conference. Separate specific instructions may be required for the guard force.

Counter Terrorist Measures

051722. When the threat from terrorism is assessed as significant, the CSO, or EsyO if different, is to consult PSyA security staff on any extra precautions deemed necessary for the conference.

This page intentionally left blank.

SECTION XVIII
TO CHAPTER 5

SECURITY OF EQUIPMENT

General

Introduction

051801. The aim of this Section is to provide advice that allows heads of establishment sufficient flexibility to decide on the protective measures to be applied to the security of equipment according to the following:

a. The assessed threat.

b. The level of protective marking.

c. Any specific vulnerabilities.

Further Information, Advice and Guidance

051802. The following information, advice and guidance on security of equipment and matrices can be obtained:

a. Establishments should seek advice, where required, on any aspects of the use of the security of equipment minimum baseline measures matrix from PSyAs.

b. PSyAs should contact DDef Sy for policy clarification on any matters arising from the security of equipment.

c. Further information regarding equipment deployed on operations can be found in Chapter 14 of this manual.

d. More information on matrices is contained in Section I to this Chapter.

e. Further information on risk management can be found in Chapter 3.

Definition of Equipment

051803. The definition of equipment in the context of applying security measures is divided into the following categories:

a. Small items of equipment that could be housed inside security containers or secure/strong rooms.

b. Large items of equipment that could be kept inside special-to-type buildings such as garages or hangars.

c. Large items of equipment that would be kept in the open on a parking, dispersal or storage area.

The Use of a Matrix

Methodology

051804. The security of equipment minimum baseline measures matrix follows the same methodology of the matrix and menu system for the security of protectively marked documents detailed in Section I to this Chapter.

Small Items of Equipment

051805. Small items of equipment follow the same rules as for protectively marked documents. The matrix in Section I to this Chapter is to be used to assess small items of equipment in the same way as if they were documents; however, larger items of equipment are catered for under different arrangements using the matrices in this Section.

The Security of Equipment Minimum Baseline Measures Matrix

The Threat

051806. The security of equipment minimum baseline measures matrices are designed to provide an appropriate level of protection for equipment against the **ESPIONAGE** rather than the terrorist or sabotage threats; however by their very nature, many large items of equipment are very valuable in financial and operational terms and the matrix provides for these factors. The system is aimed to be flexible enough to cover operational deployments and not only protection at the home base. The assumed threat level for the use of the matrix is **LOW (L)** unless otherwise directed by PSyAs having been so advised by DDef Sy e.g. The threat level for Special Armour is set at **SIGNIFICANT**.

Risk Management and Minimum Baseline Objectives

051807. Risk management offers a high degree of flexibility in providing the levels of protection required to safeguard protectively marked equipment. To ensure that there is some degree of consistency and mutual assurance about the way one establishment's assets are handled by another, certain minimum baseline objectives apply to all areas of protective security. They are intended to provide **acceptable** security at all levels of protection where the threat is assessed as **Low**, with enhanced security at levels above this baseline.

Matrices

051808. There are 2 separate matrices corresponding to the categories of **large items of equipment kept in special-to-type buildings** and **large items of equipment kept in the open**; when assessing small items of equipment the minimum baseline measures matrix shown in Section I to this Chapter is to be used. The matrices for large items of equipment are at Annexes A and B. The matrices share a common menu of measures which is at Annex C.

Range of Options

051809. The security of equipment matrices and menu of minimum baseline measures provide a range of options which meet the baseline objectives. They are designed to help the management of security risks by offering a means for the identification and selection of the most suitable and cost-effective physical security measures to safeguard protectively marked equipment against attempts to acquire them illicitly by surreptitious attack or theft. Although many of the measures suggested will be helpful in a counter-terrorist context (and suitable counter-terrorist measures already in place may, of course, be taken into account in meeting the baseline measures), the weighting given to the measures in the matrices is **not** primarily intended to meet terrorist threats.

Threat Levels

051810. The security of equipment minimum baseline measures are those in the first column of each of the matrices (headed L). The remaining columns offer a means of deciding on the increased measures appropriate to levels of threat higher than Low. Establishment security officers (ESyOs) are to keep themselves regularly up-to-date on the nature and levels of threat to their assets (by consulting their appropriate PSyAs and local Service/civil police authorities); and are to decide for themselves on the proper response to increased levels of threat, in the light of local circumstances.

About the Matrix

051811. The security of equipment minimum baseline measures are set as numerical values within each matrix, which correspond to the level of protectively marked equipment and to the level of the threat. The matrices, as shown at Annexes A and B, are supported by a menu of physical security measures (Annex C) from which measures can be selected so that the sum total of the value of the individual measures equals or exceeds the required numerical value of the appropriate minimum baseline measures. It is a fundamental principle that points are only valid when correct security procedures and practices accompany the selected measure.

Numerical Values

051812. The numerical value of the baseline measures required for each level of the protective marking system is made up from different sections of the menu of measures; some from mandatory sections of the menu of measures and the remainder from any of the sections. This system of mandatory and additional measures is to ensure that a sensible balance of measures is achieved and allows ESyOs flexibility in the measures

they apply to reach the baseline position, taking into account the security facilities, equipment and manpower at their disposal.

How the Matrix is Used

051813. Each of the matrices, depending on the category of equipment, is used by selecting the appropriate level of protectively marked equipment and then reading off the scores to be achieved against the mandatory and additional sections of the menu of measures. Having identified the points score required, the user should then turn to the menu of measures. Minimum baseline measures matrix checksheets for use by ESyOs are at Annexes D and E (depending on where the equipment is stored). A guide to the use of the security of equipment minimum baseline measures matrix is at Annex F and samples of how to complete the full documentation are at Appendices 1 and 2 to Annex F.

Security of Equipment Menu of Measures

Sections

051814. The menu of measures is divided into 7 Sections, each dealing with a particular aspect of security (or layer of 'the defence in depth)'. For ease of application, the menu is laid out as a proforma with numerical allocations provided; there are also spaces for inserting the various points scores.

Weighting of Measures

051815. Some measures are weighted in that their points score multiples with that of another measure (eg containers and locks), whilst others are added (eg fences, perimeter intruder detection systems, lighting and CCTV). The value of zero is used as a multiplier where a fence has no control of entry at its entry/exit points. Where control of entry is provided, the multiplier x 1 will validate the points awarded to the fence.

Selection of Measures

051816. In deciding what measures to select, the user is to include existing security measures and then fill in the score. The results can then be compared with the requirements of the matrix. From the comparison it will be apparent whether the measures are excessive, adequate or need 'topping up'.

Additional Measures

051817. If additional measures are required, establishments are to decide which measures to select in the light of the actual threats faced by them. If there is a threat from forcible attack, for instance, the strength of a container/casing may be a higher factor than the Class of lock; conversely, if the threat is from surreptitious attack, a high Class lock may be a more important factor than the strength of the container/casing. Used in this way, with imagination and common sense, the menu will help ESyOs to

find the measures most appropriate to their particular situation, the threats they face and the resources available.

Physical Security Measures - Performance Standards

051818. The performance standards to be used in the security of equipment minimum baseline measures matrix are those detailed in para 05113 - 05128. However the following differences should be noted.

a. **Guards and IDS (security of equipment matrix section 5).** In addition to the types of patrols detailed in para 05122, the security of equipment has 2 further types as follows:

(1) **Point guard.** A person specifically detailed to guard a particular building or individual piece of equipment continuously. The guard must be in the immediate vicinity and carry out continuous surveillance of the building or equipment to be guarded. The guard must be in possession of or have immediate access to communication equipment linked to the response force.

(2) **Dog patrol.** A patrol comprising a trained handler and trained military/Police guard dog who have successfully completed instruction at a recognised dog training school (i.e the Defence Animal Centre or MDP Wethersfield). The patrol must work within a pre-determined patrol area that is known to the guard force, and is no larger than can be reasonably expected to be covered by a single dog team. The patrol should remain continuously on their designated area until relieved or a designated time. Patrols are to be in accordance with the accepted norms for patrol durations. The handler must be in possession of communication equipment linked to the response force.

Note: The MBMM points attracted by dog patrols may not be a constant factor throughout a given period eg the patrols may only operate at night.

b. **Immediate dispersal/parking/storage area (security of equipment matrix section 6).** This is an additional section required for the security of equipment matrix; however the standards detailed in paras 05124 - 05128 apply.

c. **Outer perimeter (security of equipment matrix section 7).** The standards that apply to this section are also detailed in paras 05124 - 05128.

Movement of Protectively Marked Equipment

Movement Security Plan

051819. A movement security plan is to be drawn up prior to moving protectively marked SECRET or above large items or consignments of equipment, or other equipment with national caveats. This does not apply to equipment being carried on the

person. The movement security plan is to be drawn up by the relevant Movements Authority in conjunction with, and approved by, the consignor's PSyA in consultation with appropriate security staff and is to cover the following, as appropriate:

a. Description of the equipment, together with protective marking.

b. Details of the consignor or other authority responsible for initiating the move.

c. Name and address of the consignee.

d. Anticipated date of despatch and arrival.

e. Proposed method of movement, including details of the route where necessary, overnight storage arrangements and the name of the carrier.

f. Storage on the route.

g. Requirement for supervision of loading and unloading.

h. Contingency procedures to be adopted in the event of accident, breakdown, diversion or other delay.

i. Unusual features requiring special handling or storage.

j. Measurements and weight of consignments.

k. How packed.

l. Arrangements for customs examination and sealing.

m. Details of guards.

n. Method of transmission of keys.

Periodic movement of similar equipment between the same parties on the same route can be incorporated in one movement security plan, but otherwise a separate plan is to be made for each movement.

Distribution of Plan

051820. A copy of the movement security plan is to be sent in advance to the consignee. Relevant extracts from the plan are to be provided to the driver of the consignment.

Packaging

051821. Equipment marked CONFIDENTIAL or above is to be concealed, as far as practicable, in an anonymous covering or container. The protective marking is not to be disclosed on the covering or container. Where practicable, the equipment and its

covering/container should be in the locked body of the vehicle. When being transported in conjunction with UNCLASSIFIED or RESTRICTED material, equipment marked CONFIDENTIAL or above is to be physically separated from it by an inner lockable cage or similar barrier.

Escorts

051822. In addition to the driver, an escort is to be provided on each vehicle carrying protectively marked material of CONFIDENTIAL or above. An escort or driver is to remain with the vehicle at all times.

Communication

051823. Each vehicle on which material protectively marked CONFIDENTIAL or above is being carried, is to have a two-way communication system easily accessible to the driver/escort for use in emergencies.

Vetting

051824. Drivers and escorts of equipment protectively marked SECRET or above are under the control of a person who is suitably cleared.

Rail Movement

051825. TOP SECRET equipment is not to be transported by rail. Otherwise, the principles underlying the regulations for road movement are to be applied by the PSyA in consultation with appropriate security staff when discussing the rail movement plan with the movement staff.

Sea Movement

051826. The principles underlying the regulations outlined for road movement are to be applied by the PSyA in consultation with appropriate security staff when discussing the sea movement plan with the movements staff. In addition, so far as is practicable, British owned and crewed ships should be used for the movement of CONFIDENTIAL or above material. Where this is not possible the PSyA's advice is to be sought. In any event, unescorted access to the equipment by the crew is not permitted.

Air Movement

051827. Protectively marked equipment should normally be carried in RAF or RAF chartered aircraft. The handover requirement and the requirement for escorts during the flight should be discussed with PSyAs as required. Where this is not possible, the use of diplomatic/non-diplomatic couriers should be considered.

This page intentionally left blank

ANNEX A TO SECTION XVIII TO CHAPTER 5

MINIMUM BASELINE MEASURES MATRIX FOR LARGE ITEMS OF EQUIPMENT KEPT INSIDE SPECIAL-TO-TYPE BUILDINGS

TOP SECRET	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 3	2	2	2	2	2
Mandatory - Sections 4 plus 5 **	6	6	7	7	7
Additional - Any sections #	9	11	11	14	18
Total	**18**	**20**	**21**	**24**	**28**
SECRET	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 3	2	2	2	2	2
Mandatory - Sections 4 plus 5 *	4	4	5	5	6
Additional - Any sections #	7	9	9	12	15
Total	**14**	**16**	**17**	**20**	**24**
CONFIDENTIAL	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 3	2	2	2	2	2
Mandatory - Sections 4 plus 5	3	3	3	3	3
Additional - Any sections #	4	5	7	9	13
Total	**10**	**11**	**13**	**15**	**19**
RESTRICTED	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 3	1	1	1	1	1
Additional - Any sections #	-	-	1	2	3
Total	**2**	**2**	**3**	**4**	**5**

Notes : ** Each Section must score at least 2 points.
* Each Section must score at least 1 point.
# Except Section 2

THREAT LEVELS VH - Very High
H - High
S - Significant
M - Moderate
L - Low

This page intentionally left blank

ANNEX B TO SECTION XVIII TO CHAPTER 5

MINIMUM BASELINE MEASURES MATRIX FOR LARGE ITEMS OF EQUIPMENT KEPT IN THE OPEN

TOP SECRET	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	2	2	2	2	2
Mandatory - Section 4	2	2	2	2	2
Mandatory - Sections 5 & 6 **	8	8	8	8	8
Additional - Any Sections #	6	8	9	12	16
Total	**18**	**20**	**21**	**24**	**28**
SECRET	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 4	1	1	1	1	1
Mandatory - Sections 5 & 6 **	8	8	8	8	8
Additional - Any Sections #	4	6	7	10	14
Total	**14**	**16**	**17**	**20**	**24**
CONFIDENTIAL	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 4	-	-	1	1	1
Mandatory - Sections 5 & 6 **	6	6	6	6	6
Additional - Any Sections #	3	4	5	7	11
Total	**10**	**11**	**13**	**15**	**19**
RESTRICTED	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	2	2	2	2	2
Additional - Any Sections #	-	-	1	2	3
Total	**2**	**2**	**3**	**4**	**5**

Notes: ** Each Section must score at least 2 points.
Except Sections 2 and 3

THREAT LEVELS

VH - Very High
H - High
S - Significant
M - Moderate
L - Low

This page intentionally left blank

ANNEX C TO SECTION XVIII TO CHAPTER 5

MENU OF MINIMUM BASELINE MEASURES FOR SECURITY OF EQUIPMENT

Measure			**Loading**	**Remarks**
Section 1 – Container/casing				
1.	**Container/casing:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	2	
	d.	Class 1	1	
Sub-score (ss1) = a, b, c or d				
2.	**Lock**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	2	
	d.	Class 1	1	
Sub-score (ss2) = a, b, c or d				

Section score (S1) = ss1 x ss2	**NB. Multiply**	

Measure			**Loading**	
Section 2 – Room				
3.	**Room:**			
	a.	Strong Room	4	
	b.	Strong Room	3	
	c.	Secure Room	1	
	d.	Locked Room	0	
Sub-score (ss3) = a, b, c or d				
4.	**Lock**			
	a.	Class 4	4	
	b.	Class 4	3	
	c.	Class 3	2	
	d.	Class 2	1	
	e	Class 1	0	
Sub-score (ss4) = a, b, c, d or e				

Section score (S2) = ss3 x ss4		**NB. Multiply**

Measure			Loading	Remarks
Section 3 – Building				
5.	**Strength:**			
	a.	Class 4	5	
	b.	Class 3	3	
	c.	Class 2	2	
	d.	Class 1	1	

Section score (S3) = a, b, c or d	**NB. One figure**	

Measure			Loading	Remarks
Section 4 – Control of entry to building, area or site				
6.	**Control of entry:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	2	
	d.	Class 1	1	
	e	None	0	
Sub-score (ss6) = a, b, c or d				
7.	**Visitor control:**			
	a.	Escorted	3	
	b.	Pass/badge	1	
	c.	None	0	
Sub-score (ss7) = a, b, or c				

Section score (S4) = ss6 + ss7	**NB. Add**	

Measure			Loading	Remarks
Section 5 – Guards and IDS				
8.	**Guards:**			
	a.	Point Guard	10	
	b.	Dog Patrol	8	
	c.	Frequent Internal Patrols	5	
	d.	Infrequent Internal Patrols	4	
	e.	External Patrols	3	
	f.	Resident/Site Guard	2	
	g.	Visiting Guard	1	
	h.	None	0	
Sub-score (ss8) = [(a, b, c or d)* + (e or f)*] or g* or h				
* = if applicable. Resident/site guard will only score if there has been no other score for other guards or patrols				
9.	**IDS:**			
	a.	Class 4	5	
	b.	Class 3	4	
	c.	Class 2	3	
	d	Class 1	1	
	e	None	0	
Sub-score (ss9) = a, b, or c				

Section score (S5) = ss8 + ss9	**NB. Add**	

Measure			Loading	Remarks
Section 6 – Immediate dispersal/ parking/storage area				
10.	**Fence:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	2	
	d	Class 1	1	
	e	None	0	
Sub-score (ss10) = a, b, c, d or e				
11.	**Entry control:**			
	a.	Yes	1	
	b.	No	0	
Sub-score (ss11) = a or b				

Measure			Loading	Remarks	
12.	**Random entry and/or exit searches:**				
	a.	Yes	1		
	b.	No	0		
Sub-score (ss12) = a or b					
13.	**PIDS:**				
	a.	Yes	2		
	b.	No	0		
Sub-score (ss13) = a or b					
14.	**CCTV (to appropriate standards):**				
	a.	Yes	2		
	b.	No	0		
Sub-score (ss14) = a or b					
15.	**Lighting (to appropriate standards):**				
	a.	Yes	2		
	b.	No	0		
Sub-score (ss15) = a or b					

Section score (S6) = (ss10 x ss11) + ss12 + ss13 + ss14 + ss15	

Measure			Loading	Remarks	
Section 7 – Outer Perimeter					
16.	**Fence:**				
	a.	Class 4	4		
	b.	Class 3	3		
	c.	Class 2	2		
	d	Class 1	1		
	e	None	0		
Sub-score (ss16) = a, b, c, d or e					
17.	**Entry control:**				
	a.	Yes	1		
	b.	No	0		
Sub-score (ss17) = a or b					
18.	**Random entry and/or exit searches:**				
	a.	Yes	1		
	b.	No	0		
Sub-score (ss18) = a or b					
19.	**PIDS:**				
	a.	Yes	2		
	b.	No	0		
Sub-score (ss19) = a or b					

20.	**CCTV (to appropriate standards):**				
	a.	Yes	2		
	b.	No	0		
Sub-score (ss20) = a or b					
21.	**Lighting (to appropriate standards):**				
	a.	Yes	2		
	b.	No	0		
Sub-score (ss21) = a or b					

Section score (S7) = (ss16 x ss17) + ss18 + ss19 + ss20 + ss21	

TOTAL SCORE is the sum of SECTIONS 1 to 7	

This page intentionally left blank

ANNEX D TO SECTION XVIII TO CHAPTER 5

MINIMUM BASELINE MEASURES MATRIX - POINTS CHECKSHEET FOR LARGE ITEMS OF EQUIPMENT KEPT INSIDE SPECIAL-TO-TYPE BUILDINGS

Reference:	

Assessment		
1.	Asset assessed:	
2.	Protective marking:	
3.	Threat level:	

Points check					
4.	**Mandatory points.**				
	Section 1.	Pts required:		Pts achieved:	
	Section 3.	Pts required:		Pts achieved:	
	Sections 4 & 5.	Pts required:		Pts achieved:	
5.	**Additional points.**				
	Any Sections.	Pts required:			
	Sections 6 & 7		Pts achieved:		
6.	**Summary of points.**				
	Total Pts required:		Pts achieved		
7.	**Remarks.**				

This page intentionally left blank.

ANNEX E TO SECTION XVIII TO CHAPTER 5

MINIMUM BASELINE MEASURES MATRIX - POINTS CHECKSHEET FOR LARGE ITEMS OF EQUIPMENT KEPT IN THE OPEN

Reference:	

Assessment		
1.	Asset assessed:	
2.	Protective marking:	
3.	Threat level:	

Points check					
4.	**Mandatory points.**				
	Section 1.	Pts required:		Pts achieved:	
	Section 4.	Pts required:		Pts achieved:	
	Sections 5 & 6.	Pts required:		Pts achieved:	
5.	**Additional points.**				
	Any Sections.	Pts required:			
	Sections 7		Pts achieved:		
6.	**Summary of points.**				
	Total Pts required:		Pts achieved		
7.	**Remarks.**				

This page intentionally left blank.

ANNEX F TO SECTION XVIII TO CHAPTER 5

GUIDE TO THE USE OF THE MINIMUM BASELINE MEASURES MATRICES AND MENU FOR THE PROTECTION OF PROTECTIVELY MARKED EQUIPMENT

First actions

1. Produce a proforma that consists of the following documents:

   a. A minimum baseline measures matrix (either Annex A or Annex B as appropriate for where the equipment is stored).

   b. A menu of minimum baseline measures (Annex C).

   c. A points checksheet (either Annex D or Annex E as appropriate for where the equipment is stored).

2. On the points checksheet fill in the following:

   a. Details of the asset to be assessed (for example 'Secret aircraft in hangar').

   b. The current **espionage** threat (eg 'L').

3. Using the appropriate matrix:

   a. Read off the total points required to protect the particular asset(s) at the current threat Level and write the figure on the points checksheet (eg '14' for SECRET at Low).

   b. Read off the mandatory points required for the sections and write the figures on the points checksheet (eg '8' for Sections 1 and/or 2 plus 3).

4. Turn to the menu of baseline measures to carry out the assessment. Sample assessments can be found as follows:

   a. Appendix 1 to this Annex for large items of equipment kept inside special-to-type buildings.

   b. Appendix 2 to this Annex for large items of equipment kept in the open.

Notes:

(1) **Small items of equipment.** Small items of equipment are assessed in exactly the same way as if they were documents; therefore, assessment for them is to be carried out using the minimum baseline measures matrix at Section I to this Chapter.

(2) **Summary of the classes of equipment and security measures.** Annex E to Section I of this Chapter details the Classes of security equipment, by type.

Carrying out the assessment

5. **Section 1 - container/casing.** The aim of this section is to equate the degree of protection afforded by the casing (ie skin/fabric) and locking mechanisms of the piece of equipment to that of a security container. By comparing the piece of equipment with the standards of containers detailed at para 05114, determine the class of casing that the piece of equipment equates to and write the 'loading' figure in the sub-score column (ss1); likewise, the lock/locking mechanisms fitted to the equipment should be allocated a loading (insert at ss2) in accordance with the standards at para 05115. The Section 1 score is achieved by **multiplying** the scores of the container and lock. It is likely that most scores will be low, unless there are special security provisions, and that most scores for casing and lock will only achieve one point.

6. **Section 2 - room.** If applicable, determine the class of the room that the equipment is held in using the standards at para 05116 and insert the 'loading' figure in the sub-score column (ss3); for example an unlocked room would attract 0 points. Similarly ascertain the 'loading' for the type of lock fitted to the room using the standards at para 05115 and insert at ss4; for example a Chubb Mortice lock would attract 1 point. The section score is achieved by **multiplying** the scores for the room and the lock.

Note:

(1) Establishments are to follow the spirit of the baseline measures matrix at all times. Therefore, heads of establishment are not to allow nonsensical situations to arise such as fitting a Class 4 lock to a standard office door with glass panes, in order to score more points on the matrix, which in turn would allow other normal security precautions to be dispensed with.

7. **Section 3 - building.** Using the standards at para 05118 determine the class of the building (its strength) and insert the loading score in the Section score column (S3). For example a modern building of pre-cast panels can attract 3 points.

8. **Section 4 - control of entry to building, area or site.** Determine the class of the control of entry to the building, area or site using the standards at para 05119 and

insert in the sub- score column (ss6). Decide the loading for the visitor control and insert in the sub-score column (ss7). The Section 4 score is achieved by **adding** the 2 scores together.

Example: A building where entry is allowed by the issue of keys to authorized personnel will attract 1 point. If the visitor control system is one where they are required to be escorted at all times then 3 further points would be gained. The total for the section would be 4 points.

9. **Section 5 - guards and intruder detection systems (IDS).** The type of patrols and guarding procedures are described at para 05122 and 051818:

a. Determine the type of patrols/guarding practices in the building, area and site and insert the 'loading' scores in the sub-score column (ss8). Points can be achieved for an establishment that has both internal and external patrols. Any additional resident/site guards will not attract any further points where a score has been achieved for internal or external patrols.

Example: A particular building housing the equipment may be the subject of 'frequent Internal Patrols' (gaining a loading score of 5) and be on an establishment that has 'external patrols' around the unit (gaining a score of 3). The establishment may also have a 'Site Guard' at the incident room or guardroom. The latter would only attract points if there were no internal or external patrols. Hence the total sub-score (ss8) in this example would be 8 points.

b. Determine the sub-score for the type of IDS on the establishment, area and/or site using the standards at para 05123 and insert at (ss9).

The Section 5 score is obtained by **adding** the scores for guards and IDS and inserting at (S5).

10. **Section 6 - Immediate dispersal/parking/storage area.** Decide what Class the fence is using the standards at paras 05124 and shown by type at Section I, Annex E and insert the 'loading' into the sub-score (ss10); eg an approved 2.4 metre high chainlink fence with security topping would merit 2 points. If the establishment has entry control insert 1 point at (ss11); if it does not then no points are allotted. Similarly, insert the 'loading' figures for the 'yes/no' measures for searches (ss12), perimeter intruder detection systems (PIDS) (ss13), CCTV (ss14) and lighting (ss15). The total score (S6) for perimeter measures is obtained by **multiplying** the 'loading' scores of the fence and entry control and then **adding** this figure to the total of the rest of the sub-scores.

Example: Armoured vehicles are located in a storage area without any measures other than security lighting. The total points for section 6 would be 2.

11. **Section 7 - Outer perimeter.** Decide what grade the establishment outer perimeter fence is using the standards at para 05124 and shown by type at Section I Annex E and insert the 'loading' into the sub-score (ss16); eg an approved 2.4 metre

high chainlink fence with security topping would merit 2 points. If the establishment has entry control insert 1 point (ss17); if it does not then no points are allotted. Similarly, insert the 'loading' figures for the 'yes/no' measures for searches (ss18), perimeter PIDS (ss13), CCTV (ss14) and lighting (ss15). The total score (S7) for outer perimeter measures is obtained by **multiplying** the 'loading' scores of the fence and entry control and then **adding** this figure to the total of the rest of the sub-scores.

Example: An establishment has a Class 2 fence (2 points), with entry control (1 point). Entry/exit searches are carried out by guards (1 point) but the establishment does not have any PIDS (0 points). It also does not have any CCTV (0 points) or security lighting to the appropriate standards (0 points). The total points for Section 7 would be as follows:

Fence	x	Entry Control	+	Total of other sub-scores	=	3
(2)	x	(1)	+	(1)	=	3

Note: It is important to note that points for CCTV and lighting can only be obtained if the equipment reaches the appropriate approved standards.

Completing the points checksheet and further action

12. **Completion of the checksheet.** After completing the baseline measures menu, complete the points checksheet by inserting the total points achieved. In addition, insert the points obtained in the 'Mandatory' sections.

13. **Action to be taken if 'points required' baseline is exceeded.** If all of these figures exceed the 'points required' then the equipment has adequate security and no further action is required. However, there may be scope for the ESyO, in consultation with the head of establishment, to reduce some security measures, if desired, to the baseline position; this type of review is to be actively encouraged so long as expenditure is not wasted in the pursuit of lower standards when those in force are cost-effective already. Any agreed action could be written in the 'Remarks' column of the checksheet.

14. **Action to be taken if 'points required' baseline is not reached.** If the points achieved figures have failed to reach the points required for either the total or mandatory section scores, then the ESyO in consultation with the HOE must re-examine the security measures implemented on the establishment and choose higher security measures accordingly to meet the baseline position.

15. **Flexibility of the matrices.** The advantage of the baseline measures matrices is that they allow establishments the flexibility to choose their own security measures at a given threat level as long as the baseline position is reached and certain mandatory measures are met. They also take into account any enhanced security measures that the unit may have invested in, such as AACS, CCTV or security lighting, thereby perhaps allowing the establishment to reduce its costs in other areas of security.

When to Complete a Matrix

16. **General.** A matrix must be used for all protectively marked equipment on the establishment. Where similar items of equipment are held under similar circumstances throughout the establishment only one matrix may be required to be completed for each level of protective marking. Additionally, if items of different protective markings are housed in the same special-to-type building then as long as the requirements are adequate for the highest level of protective marking, matrices for the lower levels would not be required.

17. **'Standard' loading on the matrix.** Many of the 'loadings' on the matrix/menu of measures will be identical, throughout an establishment, for each menu completed; eg, loadings which might be standard are those for the perimeter fence, entry/exit checks, entry control, guarding/patrol patterns.

18. **Change in threat level.** If the threat changes, the ESyO should consult the completed points checksheet and menu of measures to see if the measures in force are still adequate or, in the case of a decrease in threat, whether certain measures can be changed or dispensed with. By trying differing options within the menu for a given protected asset, the ESyO should be able to obtain any new baseline position.

Example: The threat increases from Low ('L') to Moderate ('M') and the number of points required to house TOP SECRET protectively marked material increases from 18 to 20. Assuming that a particular establishment has the minimum 18 points and meets the mandatory points (which would not change for such an increase in threat) it could meet the new baseline position by introducing 'Infrequent Internal Patrols' to the existing 'External Patrols' thereby gaining the extra points required. Alternatively, it could choose to house all of its TOP SECRET equipment in a higher class of building which would meet the new baseline position.

This page intentionally left blank

APPENDIX 1 TO ANNEX F TO SECTION XVIII TO CHAPTER 5

MINIMUM BASELINE MEASURES MATRIX - POINTS CHECKSHEET FOR LARGE ITEMS OF EQUIPMENT KEPT INSIDE SPECIAL-TO-TYPE BUILDINGS

Reference:	STR/2032/6

Assessment		
1.	Asset assessed:	Armoured Vehicles
2.	Protective marking:	SECRET
3.	Threat level:	L

_Points check						
4.	**Mandatory points.**					
	Section 1.	Pts required:	1	Pts achieved:	2	
	Section 3.	Pts required:	2	Pts achieved:	3	
	Sections 4 & 5.	Pts required:	4	Pts achieved:	16	
5.	**Additional points.**					
	Any Sections.	Pts required:	7			
	Sections 6 & 7		Pts achieved:	5		
6.	**Summary of points.**					
	Total Pts required:	14	Pts achieved	26		
7.	**Remarks.**					
STANDARD OF SECURITY REQUIRED WILL MEET THREAT TO VH LEVEL						

This page intentionally left blank.

Minimum Baseline Measures Matrix for Large Items of Equipment kept inside Special-to-Type Buildings

TOP SECRET	**L**	**L**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 3	2	2	2	2	2
Mandatory - Sections 4 plus 5 **	6	6	7	7	7
Additional - Any sections #	9	11	11	14	18
Total	**18**	**20**	**21**	**24**	**28**
SECRET	**L**	**L**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 3	2	2	2	2	2
Mandatory - Sections 4 plus 5 *	4	4	5	5	6
Additional - Any sections #	7	9	9	12	15
Total	**14**	**16**	**17**	**20**	**24**
CONFIDENTIAL	**L**	**L**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 3	2	2	2	2	2
Mandatory - Sections 4 plus 5	3	3	3	3	3
Additional - Any sections #	4	5	7	9	13
Total	**10**	**11**	**13**	**15**	**19**
RESTRICTED	**L**	**L**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 3	1	1	1	1	1
Additional - Any sections #	-	-	1	2	3
Total	**2**	**2**	**3**	**4**	**5**

Notes: ** Each Section must score at least 2 points.
* Each Section must score at least 1 point.
# Except Section 2

THREAT LEVELS

VH - Very High
H - High
S - Significant
M - Moderate
L - Low

This page intentionally left blank

MENU OF MINIMUM BASELINE MEASURES FOR SECURITY OF EQUIPMENT

Measure			Loading	Remarks
Section 1 – Container/casing				
1.	**Container/casing:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	(2)	*Vehicle panels*
	d.	Class 1	1	
Sub-score (ss1) = a, b, c or d				*2*
2.	**Lock**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	2	
	d.	Class 1	(1)	*Vehicle locks*
Sub-score (ss2) = a, b, c or d				*1*

Section score (S1) = ss1 x ss2	**NB. Multiply**	*2*

Measure			Loading	
Section 2 – Room				*Not applicable*
3.	**Room:**			
	a.	Strong Room	4	
	b.	Strong Room	3	
	c.	Secure Room	1	
	d.	Locked Room	0	
Sub-score (ss3) = a, b, c or d				
4.	**Lock**			
	a.	Class 4	4	
	b.	Class 4	3	
	c.	Class 3	2	
	d.	Class 2	1	
	e	Class 1	0	
Sub-score (ss4) = a, b, c, d or e				

Section score (S2) = ss3 x ss4		**NB. Multiply**

Measure			Loading	Remarks
Section 3 – Building				
5.	**Strength:**			
	a.	Class 4	5	
	b.	Class 3	(3)	*Pre cast panels*
	c.	Class 2	2	
	d.	Class 1	1	

Section score (S3) = a, b, c or d	**NB. One figure**	*3*

Measure			Loading	Remarks
Section 4 – Control of entry to building				
6.	**Control of entry:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	2	
	d.	Class 1	(1)	*Key issue*
	E	None	0	
Sub-score (ss6) = a, b, c or d				*1*
7.	**Visitor control:**			
	a.	Escorted	(3)	
	b.	Pass/badge	1	
	c.	None	0	
Sub-score (ss7) = a, b, or c				*3*

Section score (S4) = ss6 + ss7	**NB. Add**	*4*

Measure			Loading	Remarks
Section 5 – Guards and IDS				
8.	**Guards:**			
	a.	Point Guard	10	
	b.	Dog Patrol	8	
	c.	Frequent Internal Patrols	(5)	
	d.	Infrequent Internal Patrols	4	
	e.	External Patrols	(3)	
	f.	Resident/Site Guard	2	
	g.	Visiting Guard	1	
	h.	None	0	
Sub-score (ss8) = [(a, b, c or d)* + (e or f)*] or g* or h				8
* = if applicable. Resident/site guard will only score if there has been no other score for other guards or patrols				
9.	**IDS:**			
	a.	Class 4	5	
	b.	Class 3	(4)	Approved System
	c.	Class 2	3	
	d	Class 1	1	
	e	None	0	
Sub-score (ss9) = a, b, or c				4

Section score (S5) = ss8 + ss9	**NB. Add**	12

Measure			Loading	Remarks
Section 6 – Immediate ~~dispersal/ parking~~/storage area				
10.	**Fence:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	2	
	d	Class 1	1	
	e	None	(0)	
Sub-score (ss10) = a, b, c, d or e				0
11.	**Entry control:**			
	a.	Yes	1	
	b.	No	(0)	
Sub-score (ss11) = a or b				0

Measure			Loading	Remarks
12.	**Random entry and/or exit searches:**			
	a.	Yes	1	
	b.	No	(0)	
Sub-score (ss12) = a or b				*0*
13.	**PIDS:**			
	a.	Yes	2	
	b.	No	(0)	
Sub-score (ss13) = a or b				*0*
14.	**CCTV (to appropriate standards):**			
	a.	Yes	2	
	b.	No	(0)	
Sub-score (ss14) = a or b				*0*
15.	**Lighting (to appropriate standards):**			
	a.	Yes	(2)	
	b.	No	0	
Sub-score (ss15) = a or b				*2*

Section score (S6) = (ss10 x ss11) + ss12 + ss13 + ss14 + ss15	*2*

Measure			Loading	Remarks
Section 7 – Outer Perimeter				
16.	**Fence:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	(2)	*Chainlink*
	D	Class 1	1	
	E	None	0	
Sub-score (ss16) = a, b, c, d or e				*2*
17.	**Entry control:**			
	a.	Yes	(1)	
	b.	No	0	
Sub-score (ss17) = a or b				*1*
18.	**Random entry and/or exit searches:**			
	a.	Yes	(1)	
	b.	No	0	
Sub-score (ss18) = a or b				*1*
19.	**PIDS:**			
	a.	Yes	2	
	b.	No	0	
Sub-score (ss19) = a or b				*0*

20.	**CCTV (to appropriate standards):**				
	a.	Yes	2		
	b.	No	(0)		
Sub-score (ss20) = a or b				0	
21.	**Lighting (to appropriate standards):**				
	a.	Yes	2		
	b.	No	(0)		
Sub-score (ss21) = a or b				0	

Section score (S7) = (ss16 x ss17) + ss18 + ss19 + ss20 + ss21	3

TOTAL SCORE is the sum of SECTIONS 1 to 7	26

This page intentionally left blank

APPENDIX 2 TO ANNEX F TO SECTION XVIII TO CHAPTER 5

MINIMUM BASELINE MEASURES MATRIX - POINTS CHECKSHEET FOR LARGE ITEMS OF EQUIPMENT KEPT IN THE OPEN

Reference:	STR/2033/6

Assessment		
1.	Asset assessed:	Aircraft on dispersal
2.	Protective marking:	SECRET
3.	Threat level:	L

Points check						
4.	**Mandatory points.**					
	Section 1.	Pts required:	1	Pts achieved:	1	
	Section 4.	Pts required:	2	Pts achieved:	3	
	Sections 5 & 6.	Pts required:	4	Pts achieved:	13	
5.	**Additional points.**					
	Any Sections.	Pts required:	7			
	Sections 7		Pts achieved:	3		
6.	**Summary of points.**					
	Total Pts required:	14	Pts achieved	20		
7.	**Remarks.**					
Standard of security provided will meet threat up to and including HIGH.						

This page intentionally left blank.

Minimum Baseline Measures Matrix for Large Items of Equipment kept in the Open

TOP SECRET	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	2	2	2	2	2
Mandatory - Section 4	2	2	2	2	2
Mandatory - Sections 5 & 6 **	8	8	8	8	8
Additional - Any Sections #	6	8	9	12	16
Total	**18**	**20**	**21**	**24**	**28**
SECRET	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 4	1	1	1	1	1
Mandatory - Sections 5 & 6 **	8	8	8	8	8
Additional - Any Sections #	4	6	7	10	14
Total	**14**	**16**	**17**	**20**	**24**
CONFIDENTIAL	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	1	1	1	1	1
Mandatory - Section 4	-	-	1	1	1
Mandatory - Sections 5 & 6 **	6	6	6	6	6
Additional - Any Sections #	3	4	5	7	11
Total	**10**	**11**	**13**	**15**	**19**
RESTRICTED	**L**	**M**	**S**	**H**	**VH**
Mandatory - Section 1	2	2	2	2	2
Additional - Any Sections #	-	-	1	2	3
Total	**2**	**2**	**3**	**4**	**5**

Notes: ** Each Section must score at least 2 points.
Except Sections 2 and 3

THREAT LEVELS

VH - Very High
H - High
S - Significant
M - Moderate
L - Low

This page intentionally left blank

Menu of Minimum Baseline Measures for Security of Equipment

Measure			Loading	Remarks
Section 1 – Container/casing				
1.	**Container/casing:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	2	
	d.	Class 1	(1)	*Aircraft skin*
Sub-score (ss1) = a, b, c or d				*1*
2.	**Lock**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	2	
	d.	Class 1	(1)	*Aircraft lock*
Sub-score (ss2) = a, b, c or d				*1*

Section score (S1) = ss1 x ss2	**NB. Multiply**	*1*

Measure			Loading	
Section 2 – Room				*Not applicable*
3.	**Room:**			
	a.	Strong Room	4	
	b.	Strong Room	3	
	c.	Secure Room	1	
	d.	Locked Room	0	
Sub-score (ss3) = a, b, c or d				
4.	**Lock**			
	a.	Class 4	4	
	b.	Class 4	3	
	c.	Class 3	2	
	d.	Class 2	1	
	e	Class 1	0	
Sub-score (ss4) = a, b, c, d or e				

Section score (S2) = ss3 x ss4		**NB. Multiply**

Measure			Loading	Remarks
Section 3 – Building				
5.	**Strength:**			
	a.	Class 4	5	
	b.	Class 3	(3)	*Pre cast panels*
	c.	Class 2	2	
	d.	Class 1	1	

Section score (S3) = a, b, c or d	**NB. One figure**	*3*

Measure			Loading	Remarks
Section 4 – Control of entry to ~~building~~, area or ~~site~~				
6.	**Control of entry:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	2	
	d.	Class 1	1	
	e	None	(0)	
Sub-score (ss6) = a, b, c or d				*0*
7.	**Visitor control:**			
	a.	Escorted	(3)	
	b.	Pass/badge	1	
	c.	None	0	
Sub-score (ss7) = a, b, or c				*3*

Section score (S4) = ss6 + ss7	**NB. Add**	*3*

Measure			Loading	Remarks
Section 5 – Guards and IDS				
8.	**Guards:**			
	a.	Point Guard	10	
	b.	Dog Patrol	(8)	
	c.	Frequent Internal Patrols	5	
	d.	Infrequent Internal Patrols	4	
	e.	External Patrols	(3)	
	f.	Resident/Site Guard	2	
	g.	Visiting Guard	1	
	h.	None	0	
Sub-score (ss8) = [(a, b, c or d)* + (e or f)*] or g* or h				***11***
* = if applicable. Resident/site guard will only score if there has been no other score for other guards or patrols				
9.	**IDS:**			
	a.	Class 4	5	
	b.	Class 3	4	
	c.	Class 2	3	
	d	Class 1	1	
	e	None	(0)	
Sub-score (ss9) = a, b, or c				***0***

Section score (S5) = ss8 + ss9	**NB. Add**	***12***

Measure			Loading	Remarks
Section 6 – Immediate ~~dispersal/ parking~~/storage area				
10.	**Fence:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	2	
	d	Class 1	(1)	_Barbed Wire
	e	None	0	
Sub-score (ss10) = a, b, c, d or e				***1***
11.	**Entry control:**			
	a.	Yes	1	
	b.	No	(0)	
Sub-score (ss11) = a or b				***0***

Measure			Loading	Remarks
12.	**Random entry and/or exit searches:**			
	a.	Yes	1	
	b.	No	(0)	
Sub-score (ss12) = a or b				*0*
13.	**PIDS:**			
	a.	Yes	2	
	b.	No	(0)	
Sub-score (ss13) = a or b				*0*
14.	**CCTV (to appropriate standards):**			
	a.	Yes	2	
	b.	No	(0)	
Sub-score (ss14) = a or b				*0*
15.	**Lighting (to appropriate standards):**			
	a.	Yes	(2)	
	b.	No	0	
Sub-score (ss15) = a or b				*2*

Section score (S6) = (ss10 x ss11) + ss12 + ss13 + ss14 + ss15	*2*

Measure			Loading	Remarks
Section 7 – Outer Perimeter				
16.	**Fence:**			
	a.	Class 4	4	
	b.	Class 3	3	
	c.	Class 2	(2)	*Chainlink*
	d	Class 1	1	
	e	None	0	
Sub-score (ss16) = a, b, c, d or e				*2*
17.	**Entry control:**			
	a.	Yes	(1)	
	b.	No	0	
Sub-score (ss17) = a or b				*1*
18.	**Random entry and/or exit searches:**			
	a.	Yes	(1)	
	b.	No	0	
Sub-score (ss18) = a or b				*1*
19.	**PIDS:**			
	a.	Yes	2	
	b.	No	0	
Sub-score (ss19) = a or b				*0*

20.	**CCTV (to appropriate standards):**				
	a.	Yes	2		
	b.	No	(0)		
Sub-score (ss20) = a or b				0	
21.	**Lighting (to appropriate standards):**				
	a.	Yes	2		
	b.	No	(0)		
Sub-score (ss21) = a or b				0	

Section score (S7) = (ss16 x ss17) + ss18 + ss19 + ss20 + ss21	3

TOTAL SCORE is the sum of SECTIONS 1 to 7	20

This page intentionally left blank

SECTION XIX TO CHAPTER 5

SITE ACCESS MANAGEMENT SYSTEMS

General

Introduction of Site Access Management Systems to the Defence Estate

051901. A number of events have focused the attention of the MOD on the need to explore all the options to improve the security of access, particularly in relation to visitors and contractors, within the Defence Estate. Allied to the need to incorporate greater use of technical security systems due to limited guarding resources, terrorist attacks and other non-terrorist incursions, the Department's security staffs have closely examined the extension of Site Access Management Systems (SAMS) within the Defence Estate.

051902. In addition, there is a need to upgrade the MOD's control of access systems. Control of access security, other than on a number of establishments that have installed SAMS, is at present predominantly based on the issue of paper passes to visitors and contractors. The passes do not have a photographic image of the bearer and the details of the visitor/ contractor are not entered on a database which can be used locally or via a network. The widespread introduction of SAMS may go some way to meeting our current and future security challenges and will put into place technology enhanced computer-based image capture systems that will serve the MOD into the digital age.

Definition

051903. A Site Access Management System (SAMS) is defined as a computer based control of access system, which incorporates digital image capture (of personnel/ vehicle registration number plates) and a database with a pass production system.

SAMS Applications

051904. SAMS computer-based digital capture products cover many security applications that are appropriate to Defence establishments and can considerably enhance the security at many of those establishments. The range of products available encompasses simple stand-alone, self-operated units for the production of a range of imaged passes (with database) to highly sophisticated wide-area network systems.

Benefits of Adopting SAMS.

051905. The introduction of SAMS, as a stand-alone system or as part of a Local or Wide Area Network (LAN or WAN), provides the following benefits:

a. **Increased Efficiency.**

(1) Reduced contractor costs by streamlining access to a site.

(2) Establishment of a database of visitors reduces processing time for initial (if notified) visits and revisits.

(3) Increased efficiency by not having to check as many people by telephone or other means. Cost savings attributable to administration of visits and contracts, reduction in the number of vetting enquiries (BC/CTC), and reduction in escort requirements.

(4) Provides potential manpower savings through possible combination of existing arrangements for producing permanent passes and for processing visitors.

b. **Deterrence Through Image Capture.** SAMS provides significant deterrence value, as visitors will have their image digitally captured. With the advent of biometric systems such as face verification there may be the perception that the captured image will be cross-referred with police and other Government databases. This will also reduce the incidence of contractor substitution and impersonation.

c. **Improved intelligence and information.** Details of where a person has visited or worked will be recorded as well as their clearance details (if any).

d. **Local and Wide Area Networks.** The potential exists (if required) to share data amongst user establishments via a central database.

e. **Reports and Post Incident Investigative Action.** SAMS has the ability to provide a wide range of reports in differing formats that are particularly useful in post-incident investigative procedures.

f. **Technological Integration With Other Systems.** It has the ability to be technologically integrated with security applications such as pedestrian turnstiles, access control, vehicle barriers and automatic number plate recognition. This allows data and images entered into the SAMS to pass seamlessly in real time to other systems. This eliminates the unnecessary re-keying of information that has already been entered into another system and

helps to overcome inconsistencies that can sometimes occur through human typographical errors.

g. **Corporate Image.** The widespread extension of SAMS will considerably improve the corporate image (both in the security and non-security context) of individual establishments and the Department as a whole. The current (predominantly paper-based) system is seen as giving an outdated and inefficient image. SAMS presents a modern high-tech corporate image compatible with the digital age.

Networking SAMS

Introduction

051906. A large number of visitors to Defence Establishments have no clearance and, in the event of any requirement for investigation, there is little or no information gathered with traditional paper systems. Even those with some form of clearance are often put through the control of access process several times for different establishments, and cross-referencing of information is impossible. This is inefficient resulting in a duplication of effort, unnecessary escorting and resulting in a lack of structured administrative and security information.

Benefits

051907. Existing SAMS users benefit from the information held on a local database as it provides a history, as well as clearance details, personal data and image for verification on each visit to a site. The information is, however, limited to each user or organisation, and there is still a large amount of duplication of effort and replication of data when one considers the number of separate databases. By having a central database which is updated by all SAMS users, each time a new visitor or contractor visits a site for the first time, staff will be able to check if there is a record elsewhere, as well as on their own database. If the benefits detailed at Para **051905** above are true for a single establishment's database then economies of scale and enhanced benefits may be achievable through aggregating all the data collected throughout the MOD.

Creation of MOD Central Database

051908. To address this situation a MOD central database has been established at DERA Farnborough. This will give HOEs an option to draw-upon and contribute to a centrally held database. Access to the database will be dependent on the user having access to a suitably configured PC, running Windows NT and with a connection to Restricted LAN Interconnect (RLI). There will be a joining fee for each terminal requiring access to the central database, together with a monthly service cost. This option can be obtained through the DGICS Catalogue (**051910** refers).

051909. HOEs are encouraged to consider the introduction of networked SAMS as both a cost-effective security enhancement for the establishment, and as a contribution to a MOD-wide co-ordinated approach to control of access.

System Procurement

Requirement for Command Security Staff Approval

051910. Whilst the initial decision on the requirement for SAMS is taken at establishment level, it is essential that the quality of system ultimately procured for the establishment is of an acceptable standard and design. This is ensured by the involvement of PSyA security staffs monitoring and approving ORs from establishments to ensure that appropriate security equipment standards are maintained. To assist with this procurement, DGICS have identified the only authorised supplier of systems to the MOD and placed their products within the DGICS Catalogue. Systems on offer from the supplier range from basic permanent pass production systems through to systems with full functionality that have the capability to be networked and which can access the MOD central database. SAMS **are not** to be purchased from sources other than DGICS as there will be no guarantee that they will be compatible with the MOD central system.

Compilation of Operational Requirement

051911. An OR is to be compiled by the ESyO after consultation with and approval by PSyA security staffs. The ESyO is to define clearly what is expected of the system. As part of the process to identify the preferred supplier of SAMS to the MOD a 'Technical Specification for the Supply Site Access Management Systems and Associated Goods and Services' (CAT/104341 - Version 2). This document is available through Special Services Group (SSG) and will asssist with the compilation of the OR and performance specification. Establishments may also call upon the assistance of TLB security specialists or SSG.

Site-Specific Surveying

051912. Before procuring any system, regardless of functionality, it is important that the ESyO arranges for a site-specific survey to be conducted. This process should use basic template designs as a basis for the survey with site-specific requirements tailored to produce the optimum system for the site within defined resources. Personnel with an engineering/security background, not merely a security background must undertake the 'technical survey', in order to fully appreciate the technical requirements site-by-site.

Audit Procedures

051913. A full audit of an installed SAMS is to be carried-out prior to commissioning. The audit is to be carried-out by professional security staff.

Special Services Group

051914. SSG are available to assist with compilation of the OR, performance specification, site survey and audit. Costs for such taskings will be borne by D Def Sy through the MOD SSG Advisory Account. Requests for SSG assistance are to be made in accordance with the instructions at Chapter 5 Section II Annexes A and F.

System Management

Terms of Reference (TORs).

051915. The SAMS system manager is to have TORs issued by the HOE.

System Security Policies (SSPs) and Security Operating Procedures (SyOPs)

051916. Appropriate SSPs and SyOPs must be issued for the system.

Consumables, Maintenance, Servicing and Training

051917. When procuring SAMS, the ESyO is to ensure that budgetary provision has been made for the provision of consumables and also takes account of the need to replace the system in future years (SAMS has an estimated system life of 8 years). In addition, he is to ensure that the Property Manager (PROM) includes the requirement to maintain/ service the SAMS in the establishment's Forward Maintenance Register. It is calculated that maintenance/ servicing currently represents 13.5% annually of capital outlay. Consideration is also to be given for the requirement to provide initial and periodic continuation training.

Pass Production

Pass Designs

051918. SAMS is a computer based control of access system, that also has the capability to produce passes. Whilst a variety of pass types can be produced, dependent on the user's needs and requirements, the following pass system template is recommended for all SAMS equipped establishments.

a. **Permanent Establishment Pass.** This will be a plastic card with a bar code facility and Watermark stripe. It is to conform to the design standards stipulated in Section IX.

b. **Daily Visitors Pass**. This will be a paper pass issued for very short-term visitors to an establishment. It will have an adhesive backing that will allow it to be attached to a coloured background which can stipulate whether the visitor is to be escorted (red) or unescorted (green). The background to the pass itself will be unique to the establishment and will have a barcode facility. The bearer's image will be in monochrome. There is the facility for the production of a vehicle permit with this pass.

c. **Longer Term (also called Event or Contractor's) Pass.** This will be a paper-based pass with the bearer's image in colour. It will be used for longer term visitors (and for opertional detachments where required) to an establishment. It will have a unique design incorporating a barcode facility. The pass can either be hot or cold sealed. There is the facility also for the production of a vehicle permit with this pass.

Retention of Passes for Contractors and Visitors

051919. All passes for contractors and visitors to MOD establishments, produced on SAMS, are to be retained on the issuing establishment. This is to be effected by the relevant guard/pass office retaining the pass and issuing them to the contractor/visitor as they come on site. The passes are to be handed back to the guard/pass office when the contractors/visitors leave the site.

Approval of Pass Design

051920. All establishment pass designs require ultimate approval from DDef Sy in accordance with the procedure laid down in **05916**.

CHAPTER 6

SECURITY OF ARMS, AMMUNITION AND EXPLOSIVES

Section III - Minimum standards for the storage of arms, ammunition and explosives

Section IV - Security of cadet forces arms and ammunition

This page intentionally left blank

SECTION I - SECURITY OF ARMS, AMMUNITION AND EXPLOSIVES

GENERAL INSTRUCTIONS

Introduction

06101. This chapter defines the minimum standards of physical security to be applied to the storage and movement of conventional arms, ammunition and explosives held by, or under the control of the MOD Defence Estate through its Crown Servants. Heads of Establishments (HOE) should be aware that if they contemplate contracting out management of armouries/ammunition stores, Crown immunity no longer applies and they will be required to comply in full with the Firearms Act 1968 and the physical standards for storage will be determined by the Civil Police. Any HOE considering this move is strongly advised to seek advice and guidance from their Principal Security Adviser (PSyA) before proceeding. This chapter does not apply to the protection of special nuclear materials (SNM) and other radioactive materials (ORM), nor does it apply to nuclear weapons, nuclear or radioactive munitions or reactor plant in the custody of the Services. It does not detail the standards for the protection of biological and chemical defence materials, advice on the protection, movement and storage of which must be obtained from DD Def Sy Phys Sy.

06102. Logistics, engineering, weapon and movement staffs have important roles in respect of the security and safety of arms, ammunition and explosives. PSyAs and their staff are to work closely with them in order to ensure that all relevant legislation and other regulations are complied with as far as is practicable in any given circumstances. To this end these instructions take account of the publications detailed below, but clearly cannot repeat them in their entirety. These publications are anyway subject to update and it is essential, therefore, that close liaison is maintained with appropriate branches.

a. Transport of Dangerous Goods by Road, Rail and Sea (JSP445).

b. The requirements contained in The Joint Service Manual of Movements (JSP 327).

c. The minimum Health and Safety Executive (HSE) physical security safety standards.

d. The physical security safety standards detailed in MOD Explosive Regulations.

e. Relevant single-Service explosive safety regulations, arms and ammunition accounting and store-keeping regulations.

f. The Firearms Acts 1968 and 1988.

06103. Where arms, ammunition and explosives merit protective marking on the basis of confidentiality the rules in Chapter 5 for the security of equipment apply.

Definitions

06104. The following definitions when used in this document apply:

a. **Ammunition and explosives.** In this chapter the term includes all forms of ammunition, explosives including detonators, pyrotechnics and anti-riot agents. Inert items on their own (eg, those components of ammunition which do not contain explosive, such as empty cartridge cases, links and chargers) are not included in this definition.

b. **Arms/Weapons and Weapon Components.** Arms consist of all man-portable weapons, including:

(1) Weapons removed from armoured fighting vehicles/helicopters.

(2) Infantry mortars.

(3) Man-portable surface-to-surface and surface-to-air missile systems.

(4) Full bore rifles, pistols, automatic fire weapons, shotguns and .22 rifles.

(5) Drill purpose (DP) weapons including permanently de-activated weapons and MOD owned replica weapons.

(6) Privately owned weapons and ammunition stored on MOD property.

(7) Flare and pyrotechnical pistols.

(8) Component or working parts of any arms, eg:

(a) Barrels.

(b) Bolts/Bolt Heads.

(c) Breech Blocks.

(d) Firing Pins.

(e) Firing mechanisms.

(f) Springs.

(g) Feed mechanism.

(h) Magazines.

(i) Magazine housings.

(j) Bayonets.

c. **Attractive to criminal and terrorist organizations (ACTO) stores.** ACTO stores are those items considered to be of immediate value to a terrorist or criminal. ACTO items are defined as follows:

(1) All arms under 20mm and associated ammunition;

(2) All single man-portable missile and rocket systems and associated missiles and rockets;

(3) All mortars less than 120mm and associated ammunition;

(4) All mines, anti-personnel grenades, explosives, explosive charges and accessories including detonation devices.

At times of AMBER and RED BIKINI Alert, extra security measures may be imposed by security staff to protect the movement of ACTO items.

d. **Non-ACTO stores.** Those other arms, munitions and explosive stores which are not defined or covered by sub-para c above.

e. **Small Arms Trainer (SAT) weapons.** The Home Office has agreed that Proof Marked SAT weapons are neither live nor DP weapons, but fall into a separate category of their own. Each PSyA is responsible for laying down the protection standards for his area of responsibility, based on the overall policy agreed with the lead PSyA on SAT (HQ Land Command G2). This means that Proof Marked SAT weapons are to be afforded protection based upon compromise affecting availability and integrity.

f. **Secure armouries and ammunition stores.** A secure armoury or ammunition store is one which complies with the minimum approved Defence Estates (DE) or Explosive Storage and Transport Committee (ESTC) structural

standards, or which has been strengthened to comparable standards, and is either:

(1) Visited externally by a guard or patrol at random intervals of not more than 1 hour when unoccupied, **or**

(2) Fitted with a Chief Inspector of Engineers (CIE)/Command Security Staff approved intruder detection system (IDS), backed by an effective response force.

DE Standard Drawings should be used for new builds and upgrades.

g. **Structurally approved armoury.** A structurally approved armoury is one which complies with the minimum approved DE structural standards, but is:

(1) Not fitted with an approved IDS.

(2) Not visited hourly by the guard force.

(3) Not permanently occupied.

DE is the approving authority.

h. **Bolt box.** A bolt box is a container approved by PSyAs as sufficiently secure for the storage of bolts/working parts. Boxes are to be secured by a security pattern mortise lock or a security padlock and robust hasp and staple. They must be bolted to the floor or wall. (A similar box, bolted to the structure of a building, may be used for the storage of .22 ammunition when approved by the command security staff.)

i. **Establishment Armament Officer (EAO).** This is a generic term that includes:

(1) Ammunition Technical Officer (ATO)/Senior Ammunition Technical Officer (SATO) or equivalent.

(2) OC Armament Engineering/OC Weapon Engineering (OC Arm Eng/OC Wpn Eng) or equivalent.

(3) Establishment Safety Officer (ESO) or equivalent.

(4) ESO/Explosive Responsible Officer (ERO) or equivalent.

j. **Responsible person.** A responsible person, in the context of arms, ammunition and explosive checks is one of either categories shown below:

(1) At least an NCO, civilian equivalent or civilian contractor nominated by the HOE.

(2) Armoury/ammunition and explosives store personnel judged to be competent by the EAO.

k. **Arms chest.** An arms chest is an approved container for the storage of arms or ammunition. These containers are mainly used in Reserve and Cadet Forces establishments. The approved arms chests and physical security measures to be applied are detailed in Section IV.

The Threat

06105. The threat to arms, ammunition and explosives stores comes from:

a. Terrorist, nationalist, extremist and dissident organizations, groups or individuals desiring to obtain them to further their aims.

b. Criminals who wish to acquire them for profit or criminal activities.

c. Foreign Intelligence Services (FIS) seeking to acquire details of protectively marked high technology and manufacturing processes.

d. Other persons seeking to acquire them for unauthorized purposes such as sale, private collection or personal use.

e. Authorized persons who abuse the trust placed in them, for whatever reason.

The security threat is promulgated in periodic and specific threat assessments by D Def Sy.

Responsibilities

06106. D Def Sy. D Def Sy is responsible for security policy for arms, ammunition and explosives.

06107. PSyAs. PSyAs are responsible for the implementation of security policy for arms, ammunition and explosives within their respective areas of responsibility.

06108. C-in-Cs/TLB Holders. C-in-Cs/TLB Holders are responsible for ensuring that the minimum standards required by this chapter are enforced within their Commands/areas of responsibility.

06109. Heads of Establishments (HOE). HOE are to ensure that minimum standards required by this chapter are enforced at establishment level and that any additional measures required by TLB Holders are introduced. ESyOs are responsible at establishment level for advising the HOE of the interpretation and implementation of the policy for the security of arms, ammunition and explosives.

06110. Reserve and Cadet Forces. HQs of Reserve and Cadet Forces through their officers commanding, are responsible for ensuring that at least the minimum standards for the security of arms, ammunition and explosives are enforced by Reserve and Cadet personnel, in furtherance of instructions issued by PSyAs.

06111. Small arms associations. Honorary Secretaries/Chairmen of Service small arms associations, through officers in charge of Service shooting clubs, are responsible for ensuring that where appropriate, at least the minimum standards required by this chapter are strictly enforced by members of the Services small arms associations.

06112. Chief Inspectors of Explosives (CIEs). CIEs are responsible for explosives safe practices.

Security instructions

06113. Promulgation of security instructions. Each establishment having control of materiel covered by this chapter is to publish Security Standing Orders/Instructions detailing the procedures to be followed. The instructions are to be issued by the HOE. A suggested format is at Annex A.

06114. Reviews and briefings. Security instructions are to be regularly reviewed and promulgated by means of periodic briefings. The briefings are to emphasize the threat and its likely forms, and stress the need to report any suspicious matter, loss, find or security weakness.

06115. Displaying of instructions. Establishment Security Instructions relating to arms, ammunition and explosives are to be displayed as required to ensure all staff are informed.

Basic security principles.

06116. Location of arms, ammunition and explosives. The location of arms, ammunition and explosives and the storage buildings in which they are secured must be known to, where appropriate, the ESyO, Senior Police Officer (MDP), Head of Guard Force or Civil Police where they are the response force. Priority of patrolling and response force planning is to take into account the categories, relative attractiveness, and sensitivity of the respective materials.

06117. Records. Full records of holdings, use, expenditure and disposal of arms, ammunition and explosives are to be maintained in the establishment to enable accurate periodic accounting and spot checks to be carried out.

06118. Access. Access to all materials is to be controlled and permitted only to those who have a need for such access in the performance of their duties.

06119. Delay. Physical security measures are to provide sufficient delay to allow for the arrival of an appropriate response force.

06120. Alarm systems. Alarm systems are to provide warning of an attack.

06121. Supervision of arms, ammunition and explosives. The fundamental principle for the security of arms, ammunition and explosives is that when they are outside secure stores they are never to be left unattended or in the care of unauthorized persons or taken home.

06122. Armoury doors. Armoury doors are to be kept locked or bolted on the inside when individuals are working inside, and should only be opened to allow authorized entry or exit. Outward looking door viewers must be installed. There is to be a means of external communication for those working inside when the doors are locked.

06123. Storage of arms and ammunition. Ammunition is not to be stored in the same room as arms, except in the case of a Response Force where members of that force may hold a small quantity with the weapons.

06124. Guard, Fire Services and Response Force communication. Guards patrolling armouries, ammunition and explosive stores or Fire Services and Response Forces attending incidents at armouries, ammunition and explosive stores are only to use communications approved by CIEs as presenting acceptable RADHAZ and EMC hazards.

06125. Review of holdings. Holdings of weapons, ammunition and explosives are to be reviewed by HOE periodically and whenever the operational roles or training requirements change. Holdings are to be kept to the minimum consistent with the role of the establishment.

06126. Security clearance. All personnel - whether military, civilian or contract - whose duties involve regular unsupervised access to weapons, ammunition or explosives are **not** to be permitted to assume such duties until they have been subjected to a BC and full CTC clearance. Where, however, the responsible PSyA considers it justified, the vetting requirement may be increased to SC level. Where persons currently engaged in such duties do not hold at least BC and full CTC clearance, priority action should be initiated to achieve that level of security clearance.

06127. Key control. Key control is to be used as the basis of strict control of access to arms, ammunition and explosive store holdings.

Keys

06128. Issue. Keys for armouries or ammunition stores may only normally be issued to personnel authorised in writing by the HOE to draw the keys, the same person should not have access to the keys to both the armoury and ammunition store. Armoury or ammunition store keys are not normally to be issued to any individual to allow him to draw arms or ammunition alone or unsupervised.

06129. Safeguarding of keys. Instructions for safeguarding and recording the movement of keys are given in Chapter 5; these apply to keys of armouries, ammunition and explosive stores and alarm control boxes. Keys for ammunition holdings should be stored in a separate container from keys for arms stores. Combinations of digital key pads must be safeguarded to similar standards. Keys should either be secured in an appropriate security container or held in the possession of the authorised person.

Response force

06130. Related Instructions. Paragraphs 06131 to 06134 below are to be read in conjunction with Chapter 5 Section VIII (Guards and Patrols).

06131. Regular Service Establishments. All Regular Service establishments with armouries and/or ammunition and explosive stores are to provide a response force that is capable of being armed (which must be armed if arming has been ordered) and that will react in sufficient time, taking account of the delay provided by the building construction and other physical security measures, to prevent the loss of or damage to the weapons, ammunition or explosives being protected.

06132. Other MOD Establishments. All other MOD establishments with armouries and /or ammunition and explosive stores not guarded by Service Personnel or MDP are to have contingency plans which provide a response force capable of being armed that may include the Civil Police, and which will react in sufficient time, taking account of the delay provided by the building construction, to prevent the loss of or damage to the weapons, ammunition or explosives being protected. The decision as to whether the response force is to be armed, if provided by the Civil Police, will rest with the Chief Constable of the force involved.

06133. Preparation and practice of plan. The contingency plan is to be prepared by the establishment in consultation with the Civil Police, who are to hold copies of the plan. The plan is to be practised at least annually. Notification to the correct Civil Police agency is essential, and they should be invited to attend or send a liaison officer, although their absence is not to stop the practice from taking place.

06134. *Spare.*

Patrols

06135. In addition to checks being made at prescribed intervals with the occupants of the stores/armouries when in use, (the precise timings to be decided by the HOE), regular armouries and ammunition and explosive stores are to be externally patrolled with the following frequency when they have ACTO items stored in them:

a. **Buildings with IDS.** Not required where an approved IDS is installed unless a higher alert state exists.

b. **Buildings without IDS.** At intervals not exceeding one hour.

c. **Temporary storage on vehicles.** To be covered by a portable IDS or guarded.

Issue and return

06136. A record is to be maintained of all arms issued from armouries and small arms stores and ammunition and explosives from store. A signature or tally is to be obtained from the recipient of any weapon or ammunition and explosive that is issued. On return, receipt is to be acknowledged by the person receiving the weapon or ammunition or explosive into the armoury/store as appropriate. Records of issue and return of arms and ammunition or explosives are to be retained for at least 36 months after the last entry.

Registers

06137. All arms and ammunition and explosives on charge to an establishment are to be listed in the appropriate registers and ledger. Records are also to be kept of all daily issues and receipts and these records are to be retained for at least 36 months after the last entry - these records will be subject to checking during protective security inspections.

Checks

06138. Principles. The following principles apply for the checking of arms, ammunition and explosives:

a. PSyAs are responsible for issuing instructions for the physical checking of stocks of arms, ammunition and explosives. Checks are to be recorded in dedicated logs which are to be inspected every 6 months and kept for 36 months.

b. All checks are to be carried out by a responsible person (as defined at 06104j above). The responsible person is to be someone other than those allowed unsupervised access. Thus, the armourer or arms storeman must not carry out these checks. The orderly officer of the day or similar is an appropriate person.

c. Those involved in checking are to ensure that, where bulk stocks are involved, the seals on boxes are inspected. If discrepancies are confirmed, the fact is to be immediately brought to the attention of the ESyO (see Annex B).

d. Arms, ammunition and explosives in loose form are to be accurately counted, the quantities agreed with the stock record cards and, where possible re-sealed in containers.

e. Issues, receipts and expenditure documentation are to be examined to ensure they are accurate and that transactions have been correctly authorized.

f. All arms and main stockholdings of ammunition and explosives are to be subject to regular audit and unannounced 'spot checks' by individuals other than arms/ammunition storeman.

06139. IDS. Functional checks of armoury and ammunition and explosive store IDS are to be carried out as follows:

a. **Daily checks.** A daily functional check of the IDS is to be carried out.

b. **Weekly checks.** 25% of the IDS sensors (on rotation) are to be activated by on-site personnel each week.

A record of these checks is to be maintained and these records inspected during protective security inspections.

Note: The above will apply to establishments where the alarm terminates internally, ie on the establishment. Where the alarm terminates externally, ie at a central monitoring unit, an appropriate checking system must be included in the contract.

06140. *Spare*

Losses and recoveries

06141. Arms, ammunition and explosives. All losses or recoveries of arms, ammunition and explosives and attempts to steal from or break into armouries or vehicles containing arms, ammunition and explosives (whether successful or not) are to be reported, by the fastest means available, in accordance with Annex B to:

a. The ESyO (who is to notify the MDP/Civil Police where appropriate).

b. The HOE.

c. Appropriate security unit (Area Security Team, MI Bn, RAF P&SS, CBSy, DLO or DPA security organisation).

d. Appropriate PSyA.

e. For the Navy & Army only; CCRIO RMP.

f. For the Royal Marines only; CGRM.

g. EAO/SATO.

This requirement includes any confirmed deficiencies or surplus discovered during checks.

06142. Keys. The loss or compromise of armoury/magazine keys is to be reported in accordance with Annex C to the following:

a. The ESyO.

b. The HOE.

c. Appropriate PSyA and appropriate local security unit.

d. For the Royal Marines only; CGRM.

e. EAO/SATO.

06143. The PSyA will decide whether an investigation is required and the agency best suited to conduct it. Investigation reports are to be forwarded to the PSyA for further action or case closure.

Materials on loan

06144. Loans of material between establishments or to industrial firms are to be formally approved by line management responsible for the material. The loan must be documented and must specifically state the period of loan and the responsibility of the recipient to provide security protection on delivery. The appropriate officer is to be satisfied that effective safeguards exist and that the transfer is correctly authorized and documented. Where loans are to be for long periods (one year or more) the recipient is required to confirm that the materials are still held by him and correctly stored on a 6 monthly basis, or that the materials have been expended.

06145. *Spare.*

Drill Purpose (DP) and MOD owned Replica weapons

06146. Drill Purpose (DP) and MOD owned replica weapons are to be stored securely as detailed at sub-para 06134i below. They are not normally to be stored in Service Armouries. (When large numbers are involved a Class 3 or Class 4 IDS is to be fitted).

ANNEX A TO SECTION I TO CHAPTER 6

SUBJECTS TO BE COVERED IN ESTABLISHMENT SECURITY INSTRUCTIONS FOR THE PROTECTION OF ARMS, AMMUNITION AND EXPLOSIVES

1. Name, location and telephone no of the Establishment Security Officer.

2. Scope of the instructions.

3. The security threat.

4. Security responsibilities:

   Security Officer, Explosives/Safety Officer, Armament Officer, Production Manager, Transport Officer, heads of Departments, Stores/Supply Officers, Foreman in Charge of Operations/Accounting/Movement, Explosives Workers.

5. Security procedures to be followed in production/process areas, storage servicing, processing, trials, quality assurance, climatic and other tests or other activities in respect of arms, ammunition and explosives.

6. Control of access to buildings, areas, compounds.

7. Control of security keys - in use and duplicate.

8. Accounting - audit and spot checks.

9. Security education and briefings of staff.

10. Action on discovery of a loss/surplus.

11. Details of response force arrangements (e.g. size, response time, orders, activation and deployment).

12. Actions to be taken in response to activation of alarms (e.g. duress situations).

This page intentionally left blank

ANNEX B TO SECTION I TO CHAPTER 6

REPORT FORMAT FOR THE LOSS, RECOVERY OR ATTEMPTED THEFT OF COMPLETE ARMS, AMMUNITION OR EXPLOSIVES

A Establishment, name of person reporting, contact telephone number.

B Item identification: type, calibre, make, nature, description.

C Quantity: numbers or weight.

D Serial numbers (arms), batch numbers (ammunition/explosives) or other identifying marks (e.g. packing and labelling details).

E Place of loss/recovery: map sheet, grid reference, number of building or bunker.

F Outline of circumstances of loss, or recovery.

G When loss occurred and when loss was discovered.

H Action taken. Person investigating loss, the nearest Security Unit (Area Security Team, MI Bn, RAF P&SS, CBSy, DLO, DPA security organisation (who and location)). Action being taken to prevent a further loss.

I Where crime is suspected, the Service/MDP/civil police POC involved.

Notes:

1. For addressees see para 06040, Section 1, Chapter 6.

2. When sent by signal, it is to be sent under SIC YAL with a minimum PRIORITY precedence.

This page intentionally left blank

ANNEX C TO SECTION I TO CHAPTER 6

FORMAT FOR REPORTING LOSS OR COMPROMISE OF KEYS TO ARMOURIES AND MAGAZINES

Subject: Loss/compromise of armoury/magazine keys

A. Establishment, name of person reporting, contact telephone number.

B. Contents of armoury/magazine.

C. Brief statement of circumstances.

D. Remedial action taken. (Temporary security arrangements made such as removal of arms/ammunition to secure area.)

Notes:

1. For addressees see para 06040 Section 1, Chapter 6.

2. When sent by signal, it is to be sent under SIC YAL with a PRIORITY precedence.

This page intentionally left blank

SECTION II - MOVEMENT OF ARMS, AMMUNITION AND EXPLOSIVES

Introduction

06201. These instructions are to be read in conjunction with other relevant JSPs, statutory instruments, bye-laws and other forms of delegated legislation, and explosives regulations that apply to movements of ammunition and explosives.

06202. All weapons in transit are to be treated as if they are classed within Section 5 of the Firearms Act 1968. Arms, ammunition and explosives are at greater risk when they leave the protected facilities of an establishment and are particularly vulnerable when they are being transported off main roads, during the hours of darkness and at stopping points whilst enroute.

06203. Communications giving details of the movement of arms, ammunition and explosives are to be handled on a strict 'need to know' basis and all personnel involved must be reminded of the need for discretion.

Planning of movements

06204. General. All details of the move must be protected until the latest possible moment. Normally, movement of arms, ammunition and explosives should be by the most direct authorised route, however, when regular deliveries between the same two locations are made movement arrangements should be regularly reviewed and varied, even if this could result in administrative inconvenience or additional financial cost. Details of the movement regulations for arms are held in JSP 327. Regulations for the movement of ammunition and explosives are in JSP 445. Details of procedures to be followed by Service shooting clubs and cadet forces when moving small amounts of arms and ammunition are at Section IV of this chapter.

06205. Movement plans. There is to be consultation between the officer or consignor responsible for the move and the appropriate Establishment armament and security staffs in the preparation of the movement plan. All changes to the plan are to be notified to the appropriate Security Officer.

06206. Regular moves. When arms, ammunition and explosives stores are to be moved on a regular basis and it is not possible to change routes or the pattern of movements significantly, as per para 06058 above, then PSyAs are to be consulted in the preparation of security plans. This includes any movement of such materiel to Northern Ireland. Plans should consider the following:

a. **Split consignments.** Whether the material can be sent in split consignments (i.e.weapons in one vehicle, and barrels or firing mechanisms in

another vehicle. Both vehicles dispatched at different times and via different routes).

b. **Civil Police assistance.** Notifying Civil Police forces along route.

06207. Movement of ACTO stores during BIKINI Alert States AMBER and RED. At BIKINI Alert States AMBER and RED no movement of ACTO stores (see paragraph 06004b) is to take place without first consulting Command Security Staff for advice on appropriate additional security measures. This may include delaying non-essential moves until the Alert State has decreased.

Guiding principles for the carriage of arms, ammunition and explosives by individuals

06208. The following principles are the minimum requirements to be adhered to when carrying arms and ammunition and deviations from them are only to take place in exceptional circumstances. Before implementing these principles, security staff should consult with other relevant staff branches such as movements, logistics and engineering. Security or other staffs may wish to impose tighter regulations to reflect local laws and/or the prevailing security situation. Arms and ammunition carried by individuals, whether on foot or in Service, public or private transport are never to be left unattended in any circumstances. Arms issued to individuals remain the responsibility of the individual until a recognised change of responsibility takes place. In principle, personal weapons should only be carried openly whilst on duty at Service establishments, whilst training on recognised military training areas or public or private land being used for approved training, or whilst engaged in public duties or taking part in Service displays. In all other circumstances weapons are to be handled in a manner which will not alarm the civil population and should be kept out of sight and should not be displayed in public places, eg motorway service areas, so far as is consistent with the overriding need for security of personal weapons.

a. **Service transport.** Arms and ammunition are normally to be carried in Service transport.

(1) This includes Service vehicles with civilian registration plates and contract hire vehicles.

(2) This also includes charter aircraft and ships and rail. When these are to be used, both security and movements staff are to be consulted for detailed instructions as to how arms and ammunition are to be loaded/carried.

b. **Escorts.** If an individual is to carry more than a personal weapon in a vehicle, at least one other person is to be an escort. Armament personnel carrying out maintenance at outlying armouries and cadet force units may carry up to 4 weapons and 2Kg (NEQ) of Hd 1.4 SAA in an oicial vehicle without an escort.

c. **Disabling of weapons.** Whenever possible weapons are to be disabled and working parts stored separately, although they may be in the same vehicle as the parent weapon.

d. **Visibility.** Weapons, weapon parts and ammunition are to be stowed in such a way that they are not visible or identifiable from the outside of the vehicle. Ideally weapons should be locked in the boot of the vehicle and/or be locked inside an anonymous container.

e. **Vehicle security.** All vehicle doors and, where appropriate, the boot are to be locked at all times.

f. **Separation of arms and ammunition.** Arms and ammunition are not to be carried in the same vehicle.

g. **Authorization for carriage of arms, ammunition and explosives.**

(1) Whenever a civilian registered vehicle, (including military vehicles with civilian registration), is used for transportation of arms and/or ammunition, written authority must be obtained from the HOE (for official transport), or PSyAs (for privately owned vehicles). This authority is to contain as a minimum requirement, the details of the move, the name of the vehicle driver, the vehicle registration number and the address and telephone number of the despatching unit, the type of ammunition/weapon and its serial number. A copy of this authorization together with an official identity card is to be held by the driver of the vehicle and should be presented on demand to Police or Service personnel.

(2) In exceptional circumstances when there is an urgent need to move explosive materiel and no MOD transport is available, up to 2Kg mass of explosive or explosive devices may be authorized to be carried in a privately registered vehicle by the HOE. Larger quantities may be authorized by PSyAs. A copy of the authorization, which is to include the name of the person authorized to carry the materiel, the quantity to be carried, the route to be taken, the method of transport and vehicle registration number, and a contact number in the despatching unit, is to be held by the driver and is to be presented on request to police or Service personnel.

h. **Carriage on public transport.** Unless authorized by PSyAs individuals, whether in uniform or not, are not to carry Service arms and/or ammunition on public transport. This includes trains, buses, taxis, ships and aircraft. If there is a necessity to use public transport, movements staff should be consulted in order that correct official movement channels are used rather than individuals. Dispensation from this rule will be given by PSyAs only in

exceptional circumstances and normally only after consultation with relevant police forces.

i. **Securing of materiel.** All explosive materiel should be secured out of sight in an approved container in accordance with JSP 445.

06209. In private transport. When PSyAs authorize the carriage of arms and/or ammunition in privately owned transport the following rules are additionally to be applied:

a. No more rounds of ammunition than are necessary may be carried in the same vehicle as weapons that could fire those rounds.

b. If both arms and ammunition are carried in the same vehicle, there must be at least one person accompanying the driver.

c. The validity of private insurance policies is to be confirmed.

06210. The minimum standards detailed above for the carriage of arms and ammunition by individuals is to be reviewed regularly by PSyAs, and whenever the BIKINI alert state changes.

06211. Detailed instructions are to be drawn up for action by individuals carrying arms and ammunition when involuntary delays (such as road traffic accidents) occur on journeys.

06212. Arms and explosives search (AES) teams. Team explosive samples are to be held in approved containers. Where the size and design of the vehicle allow it, the container should be securely attached to the vehicle either by bolts or steel cable and a security padlock. When operations require an overnight stay away from parent Service premises, the vehicle must be parked in an overnight staging area as defined in Paragraph 06082.

06213. Travel to/from Northern Ireland. In exceptional cases, agreed by HQNI, personnel may travel to NI with a weapon. An individual travelling to or from Northern Ireland by commercial sea/air routes is to declare his possession of weapons and weapon parts to the movement control representatives in charge of the embarkation. Secure stowage for the weapon and weapon parts will then be arranged.

06214 -06219. *Spare*

Bulk (non-individual) movement by road - general

06220. Emergency notice. A card or notice should be carried within the cab of each vehicle informing the Civil Police of an official contact should both driver and escort be injured in an accident. In addition an authority is to be carried informing the police that the driver is not permitted to leave his vehicle unattended. The driver is to take the vehicle to the nearest police station if requested to do so by the police. The relevant

documents for ammunition and explosives are as appropriate; F Mov 773, F Mov 936 a-e and authorised 'Tremcard'.

06221. Additional measures. Establishments involved in frequent or regular movement of ACTO items are to consider additional measures as follows:

a. The installation of an audible vehicle alarm approved by the CIE.

b. The fitment of an approved tracking device approved by the CIE.

06222. Need to know. The driver and escort are to ensure that they do not discuss the nature of their journey or duties with anyone who is not authorized to know and they should report as soon as possible any suspicious or untoward incident or questions raised by a member of the public.

Bulk (non-individual) movement by road - ammunition and explosives

06223. The necessary regulations are in JSP 445.

Bulk (non-individual) movement by road - arms

06224. Vehicles. All movements by road should be made in vehicles under the control of MOD or approved contractors. The vehicles should not be left unattended at any time.

06225. Contractors. Only approved contractors (who, for UK movements, hold a Section 5, Firearms Act clearance) are to be used. It is the responsibility of the establishments to consult with Command security staffs to ensure that the firm/driver/escorts have been appropriately security checked.

06226. Securing of loads. Materials carried by road vehicles should where possible be boxed or secured in lockable containers and when possible loaded in such a way as to inhibit their removal except by mechanical means. The use of MOD 'Powder Wagons' or similar enclosed box commercial vehicles, secured by approved padlocks is particularly advised. Where open flat-bed trailers are used, sheeting is recommended as screening. Consignments should be stowed in the vehicle in such a way that their contents are not obvious to the casual observer.

06227. Duplicate security keys. When regular consignments are carried by road and there are no safety requirements to check the load periodically, the following applies:

a. ISO containers are to be sealed using approved security seals.

b. Where containers with padlocks are used, duplicated security keys should be held at both the point of departure and point of delivery. However,

when access to the load is required for any safety reason and security keys must therefore accompany the load, they are to be secured on a chain and carried by the driver or escort. No additional copies of keys are to be made.

06228. Instructions and briefings. Detailed instructions and briefings are given to both driver and escort for each movement. Annexes B and C respectively provide details of points to be covered. Annex D is a specimen form of authority to be carried by the security escort/driver.

06229. Escorts. The following applies to the use of escorts:

a. Other than as indicated in this chapter an escort must always be provided for movements of arms. This means an escort in each vehicle if not travelling in an organised convoy. In organised convoys escorts are only necessary in the leading and last vehicles and in the fifth and each successive fifth vehicle. Driver or escort must carry written authority for the movement (see Annex D).

b. Where only weapon or munition 'component parts' are being carried, and the items in isolation would be of no value to a criminal or terrorist then no escort is necessary.

c. An escort is to travel in the cab of the vehicle with the driver. He is to be particularly alert to the possibility of tampering with the vehicle/load when the vehicle is stationary. Either the driver or escort is to remain with the vehicle when it is stopped.

d. A sign will be carried by the escort indicating that the occupant will not open windows or doors and showing the hazard and other details of the load but if necessary will follow a police car to the nearest police station. A contact number will also be on the sign, for police to use in case of emergency.

e. To obviate the need for escorts and enhance general security, consideration should be given to consignments of materiel being broken down to component parts and despatched separately.

06230. Communications. All vehicles and convoys involved in the bulk movement of arms are to have two-way communications easily available to the driver/escort to summon assistance in case of emergency. Following an accident to the vehicle note should be taken of the radio hazard limitations.

06231. Breakdown and accidents. If a vehicle breaks down, the civil police, the nearest Service unit and consignor are to be informed without delay. Should the vehicle be involved in an accident and the load, packaging or seals appear to be damaged, an authorized armament officer/contractor is to be called to inspect the load before anything is moved or handled. Repairs are not to be carried out in any garage until the vehicle has been unloaded under Service supervision. If it is necessary during the

course of conveyance to transfer the contents from one road vehicle to another, an authorized armament officer/contractor will be required to attend.

06232. Overnight staging. Vehicles carrying arms must be staged at Service establishments or civil police stations. Arrangements for staging are to be made by consignors before the start of a road movement. The establishments listed in JSP 445 are able to provide adequate security protection for loaded vehicles. In the event of an unscheduled overnight stop at an unlisted establishment through breakdown or other unplanned events, it is the driver's responsibility to ensure that his vehicle and contents is properly safeguarded as per sub-para 06033c above.

06233. Large/attractive consignments. The dispatching unit is to advise the appropriate single-Service security unit of the movement by road of a large or attractive consignment. The consignor will arrange for civil or Service police escorts if necessary.

06234. Routing of vehicles and arming of escorts. The routing of vehicles should, where possible and subject to safety requirements, be via Motorways and 'A' class roads. Stops for rest and food should be taken at MOD or Service establishments. Where this is not possible and stops are made at public service areas, the vehicle must be parked to allow continuous observation. Outside of MOD or service establishments an escort must stay with the vehicle at all times and be locked in the cab of the vehicle. The person absent from the vehicle must carry the vehicle keys. Normally escorts will not be armed. If the threat is such that arming of escorts is considered necessary, guidance is to be sought from PSyAs.

Bulk (non-individual) movement by rail

06235. General. Specific regulations for the movement by rail of ammunition and explosives are covered in JSP 445. All movement by rail must be by 'through' wagons and under the 'controlled service' operated by the Defence Transport and Movements Agency, Movement Control Centre (DTMA MCC), Andover, Hampshire. Rail wagons are not to be dispatched until confirmation has been given that the delivery can be made during the same working week.

06236. Packaging and loading. Within wagons materials should be packaged and where possible the wagon loaded so that it can only be unloaded by mechanical means.

06237. Alarmed wagons/containers. Rail operators may be able to provide alarmed wagons/containers. These wagons should whenever possible be used. Each wagon is to be sealed by approved security seals under the supervision of the consignor.

06238. Small consignments. All consignments under 250Kg gross should be sent by escorted Service transport; for such small quantities, a sealed rail wagon should be used only when Service transport cannot be provided.

06239. Marking of consignments Wagon-load consignments of small arms, ammunition and explosives for delivery in the UK are not to carry externally a copy of the wagon consignment note. Wagons carrying shipping consignments are to continue to carry the consignment note externally and, in such cases, the form should show only the leading shipping mark number and should not disclose details of the contents.

06240. Notification of consignee. Consignors are to advise consignees by telephone, priority signal or teleprinter message, followed by a letter sent by first class mail, of the following details:

a. Issue voucher no.

b. Brief description of consignment.

c. Consignment note no.

d. Method and the date of dispatch.

06241. Notification of DTMA MCC. In addition, consignors are to advise the DTMA MCC by telephone, priority signal, teleprinter or telex on the day prior to dispatch giving the following details:

a. Railhead from which dispatched.

b. Railhead to which dispatched.

c. The 'ready to move' date of the special train.

d. The number of wagons in each rail marshalling category.

e. The rail wagon number for single wagon consignments and at least 2 rail wagon numbers for each marshalling category when the consignment is more than 1 wagon.

f. The title and address of the consignee.

06242. Delivery and collection at railheads. Consignments will be delivered into consignee's rail sidings where possible. Where this is not possible because the consignee is not rail served, Rail operators will advise the consignee (as shown on the wagon label) that collection should be made. This is to be effected on the same day to avoid consignments remaining in sidings overnight. Consignments will be released only to properly authorized representatives presenting a letter of authority signed by an officer, clearly impressed with the unit's stamp and dated. The Rail operator's advice to consignees mentioned in this paragraph is in addition to the advice sent by DTMA MCC which will normally be received first. Consignees should not wait for the Rail operators advice before initiating action.

06243. Restriction on dispatch.

a. For security reasons it is undesirable that consignments of arms, ammunition and explosives should stand in railway sidings at weekends and during public holidays. Therefore, consignors should arrange dispatch of such traffic so that consignments arrive at their destinations and are received by consignees before weekends or public holidays. Local Rail operator representatives will advise on this matter.

b. The DTMA MCC controls the call-forward of consignments despatched to ports for overseas shipment and, in the light of up-to-date information, avoids such consignments standing in port areas longer than necessary. On receipt of call-forward instructions, consignors are to telephone the DTMA MCC for the dates of dispatch from depot or railheads.

06244. Loss or discrepancy. The following procedure is to be carried out when consignments sent by rail are not received within the time shown:

a. If the consignment has not been received by the consignee within one hour after the time advised by the DTMA MCC the latter will then take action to trace the wagon through the Rail operator and subsequently advise the consignee to take the further action shown in b. below if necessary. If the consignment has not been traced within 24 hours the consignee's superior HQ and nearest security units are to be informed.

b. When rail-wagon load consignments have not been received within 3 days of the date of despatch and cannot be traced by the DTMA MCC the consignee is to take further action as follows:

(1) Inform the nearest Civil Police Force.

(2) Make full reporting action as shown at Part 1, Paragraph 06040.

06245. Checks of consignment. On despatch and immediately on receipt rail wagons are to be examined to ensure that they are correctly locked and/or sealed. On receipt loads are also to be subjected to a 100% check and a record made of this action. Any discrepancies are to be reported to DTMA MCC.

06246. Security considerations in establishments. The location of loaded wagons within an establishment is to be reported to the Guard Force. Wagons should be positioned in the best location to facilitate security protection, checking and supervision. Consideration must be given to the adequacy of security lighting, guard dogs and 'stand alone' alarms.

Bulk (non-individual) movement by sea

06247. General. Specific regulations for the movement by sea of ammunition and explosives are covered in JSP 445. Whenever possible arms, ammunition and explosives should be carried in Service shipping or, when this is not possible, in British Shipping operating under the British Flag. If difficulties are encountered in meeting this requirement then the DTMA MCC and the Security staff are to be consulted.

06248. Responsibilities.

a. The consignor or responsible movements authority is responsible for the supervision of loading and despatch of the material. The movement of materials from the port to destinations within the United Kingdom either by road or rail is to accord with the provisions of this chapter.

b. The DTMA MCC in the United Kingdom or movements organizations overseas are responsible for providing the consignee with full details of the load, the name and type of ship, the arrival port and the estimated time of arrival.

06249. Escorts. Provision of escorts should always be considered.

06250. Sealing. Holds are to be sealed using approved seals in the presence of an authorized representative of the consignor, and opened at the destination in the presence of an authorized representative of the consignee, who is to be responsible for the supervision of the unloading and the dispatch of the consignment to the unit location. In certain circumstances the master of the vessel may require access to the sealed hold and when this occurs the authorized representative of the consignee is to ensure afterwards that the consignment has not been tampered with. Lockup stowage is always required for small arms.

06251. Personal weapons. Personal weapons taken on board vessels are normally to be labelled, stored under collective secure arrangements in the ship's armoury during the voyage and only re-issued just before disembarkation.

06252. Responsibilities. On commercial ships, the responsibility for the security and storage of arms lies with the Master of the vessel in consultation with the Commanding Officer of the embarked unit. For short voyages, individuals may retain weapons in their possession throughout the voyage. For longer voyages weapons should be stored in the most secure locker or compartment made available under arrangements of the ship's master, the Service embarkation authority and the Commanding Officer of the embarked unit. In such circumstances guarding arrangements must be considered.

Bulk (non-individual) movement by air

06253. General. Specific regulations for the movement by air of ammunition and explosives are covered in JSP 335. Ideally materiels should be carried in RAF Aircraft (and accord with Security regulations set out by the RAF) or British chartered aircraft on contract to the MOD. Where this is not possible UK civil air lines or those of the consignee's country may be used. (Civil aircraft must be registered in either the consignor's or the consignee's country). The Captain should also normally be a British national or a national of the recipient country. Flights must be direct wherever possible and must not be over communist or other countries which present a threat.

06254. Responsibilities. Where the consignor is not the Ministry of Defence it is the responsibility of the appropriate PSyA in conjunction with the consignor to determine whether air consignments need to be escorted by security escorts, and the PSyA will give guidance. A decision will be made after considering the nationality of the aircrew, the route of the flight and the current political situation in any country in which the aircraft expects to land, overfly or to which it may be diverted.

06255. Security measures. The following measures are to be taken:

a. Material delivered to the aircraft must be loaded immediately or be returned to the consignor or kept at the airfield under appropriate security protection.

b. At intermediate routine stops the material must remain in the aircraft and the department has to be satisfied that adequate safeguards are provided.

c. For an emergency landing, or prolonged delay at an intermediate stop, such effective measures for the protection of the material where possible are to be taken.

d. The aircraft must be met as it lands at its destination, and the materials delivered to the consignee (or his agent). Where this is not possible the material must be stored under acceptable and agreed security protection.

e. Where a consignment cannot go by direct flight, and trans-shipment will be necessary on route, the consignment must not be despatched until proper arrangements have been made for secure trans-shipment - eg, unloading and guarding on the ground, storage, and onward loading. Such arrangements must have the approval of PSyAs.

This page intentionally left blank

ANNEX A TO SECTION II TO CHAPTER 6 - SECURITY ASPECTS TO BE CONSIDERED IN MAKING A MOVEMENT PLAN OR PROVIDING INSTRUCTIONS OR BRIEFINGS

1. Date and time of move. (Not at night unless operationally vital)

2. Date and time of arrival.

3. Route to be followed. (Consider changing routes with consecutive consignments).

4. Planned stops for food and rest.

5. Planned stops for overnight security.

6. Provision of escorts.

7. Telephone numbers (consignor, consignee, breakdown, accident, MDP etc).

8. Procedure to be followed after breakdown or accident.

9. Reporting of movement and arrival (must report back within specified times and on arrival at destination).

10. Name of person responsible to receive consignment.

11. Ensuring consignment is checked, and signed for on arrival.

12. Procedure for receipt of materials on route.

13. Immobilization of vehicles.

14. Protection of security keys.

15. Need to request assistance from MDP or Civil Police for any particularly vulnerable part of the journey.

16. Communications requirement

.

This page intentionally left blank.

ANNEX B TO SECTION II TO CHAPTER 6

SPECIMEN FORM OF INSTRUCTIONS FOR SECURITY ESCORT/DRIVER FOR MOVEMENT OF ARMS

1. You have been appointed a security escort/driver in charge of a consignment of stores to be moved as in the attached authorization. The following paragraphs describe your responsibilities during the journey and are in addition to those required by JSP 445.

2. The route to be followed and the measures planned to safeguard the consignment will be explained to you. You will be given written details of:

a. Route.

b. Approved stopping places.

c. Destination and delivery point.

d. Accident routine.

e. Hand-over arrangements.

a. Identification of persons who may have access or who will take delivery.

g. Reporting procedures both routine and emergency.

3. You (or senior escort if a convoy is used) will be responsible for the security of the consignment until it has been handed over to the consigned, or his authorities representative, and a receipt obtained. In the event of unforeseen circumstances arising during the journey, you must institute whatever measures you may consider necessary to protect the consignment. To assist in such circumstances you will be provided with a form of written authority which should be shown to the Civil Police or Service Authorities in support of any request for assistance or additional security protection.

4. Your duties are to:

a. Take care to avoid incidents which might jeopardise the safety of the consignment.

b. Take immediate action to safeguard the consignment in the event of:

(1) Delay en route,

(2) Damage,

(3) any accident,

(4) any unplanned circumstances.

c. Ensure that no opportunity is given for unauthorized inspection, theft or malicious damage to the consignment.

5. The following specific points are brought to your attention:

a. You must examine the consignment before departure and satisfy yourself that it is complete, that it is securely packed and that its markings do not disclose the contents beyond those required when such stores are being moved.

b. You must not permit any unauthorized person to have access to the consignment or vehicle particularly when stationary or at an authorized stopping point etc. Accompanying movement documents must not leave your possession and may not be shown to unauthorized persons. Should the Civil Police wish to inspect the vehicle then they must be told to contact your establishment to obtain safety advice before doing so.

c. You must not leave the consignment unattended unless it is under constant guard by Police or Armed Forces or within the protected area of a Government establishment or on premises approved by the Authority.

d. In the event of unforeseen delay the consignor and the consignee must be informed at once. If necessary you should seek help from the authorities mentioned at c. above.

e. You must ensure that the consignment is delivered to only the consignee or his duly authorized representative. If unforeseen circumstances make it necessary to transfer the consignment, or part of it, to other than the authorized recipient you must first obtain authority to do so from the consignor.

f. On handing over the consignment you must obtain a signed receipt which must be returned to the consignor.

6. If you are in any doubt about your duties or responsibilities as a security escort you must obtain guidance before commencing the journey.

(Signature) .....…….....

(Appointment) .....……...
(Must be a responsible person as defined in para 06004.j above).

(Establishment) …….....

(Date) .....…….

(Telephone number-Civil) …….....

(Telephone number – military) ……..

This page intentionally left blank

ANNEX C TO SECTION II TO CHAPTER 6

RESTRICTED – When completed
(may be protectively marked higher if appropriate)

FORM OF AUTHORITY TO BE CARRIED BY SECURITY ESCORT/DRIVER FOR MOVEMENT OF ARMS

Valid until _____

This is to certify that

(Name) _____(Driving licence no.)_____

(Pass/ID Card No.)_____ (Travel document no.)_____

whose signature is appended below, and who is accompanied by*

(Name) _____*(Driving licence no.)_____

(Pass/ID Card No.) _____ (Travel document no.) _____

is responsible for the safe transport *(in vehicle no) _____
of a consignment of material which is the property of Her Britannic Majesty's Government. This consignment is being moved

from _____ via _____

to _____

leaving at _____ on _____

We have instructed (Name) _____ that the consignment must never be left unattended, that he/she must decline to answer questions concerning the consignment and that no unauthorized persons, except members of the Emergency Services, are to be allowed to examine the contents.

RESTRICTED – When completed)
(may be protectively marked higher if appropriate)

RESTRICTED
(may be protectively marked higher if appropriate)

It is requested that (Name) _____ may be afforded all possible facilities in the discharge of his duties. In the event of (Name) _____ suffering serious injury will the finder of this certificate please communicate at once with

Despatching unit: _____

Unit address: _____

Unit telephone number: _____

and/or notify: _____

Specimen of signature of (Name) _____

Signature of authorizing official Stamp of authority

*Insert as appropriate

List of arms by type:

RESTRICTED – When completed
(may be protectively marked higher if appropriate)

SECTION III TO CHAPTER 6

MINIMUM STANDARDS FOR THE STORAGE OF ARMS, AMMUNITION AND EXPLOSIVES

Introduction

06301. General principle. All arms, ammunition and explosives are to be stored and protected in buildings and areas that meet the MOD security and safety standards. The Defence Estates (DE) minimum standards for armoury buildings are detailed at Annex A, and those for storage of ammunition and explosives are at Annex B. Details of security locks are at Annex C to this Section.

06302. Increased protection for buildings not constructed to full security standards. Storage buildings which, because of their age, function and size, do not and cannot meet the accepted standards are to be inspected to determine an acceptable level of protection. These measures could include use of a combination of high security weldmesh fencing, additional detection devices, CCTV and approved security lighting, increased patrolling or the introduction of guard dogs (see Annex A).

06303. Security considerations. In order to minimise the financial and manpower costs establishments are to:

a. Consider the use of approved alarm systems and approved CCTV systems. (The use of a SEAP approved Class 4 IDS is mandatory for the storage of arms, ammunition and explosives that are considered to be ACTO as listed in Chapter 6 para 06104b).

b. Concentrate holding of materials in the least number of buildings commensurate with safety regulations.

c. Store ACTO materials in the most secure accommodation.

d. Consider the short-term use of an approved arms chest where the quantity of arms, ammunition and explosives is small.

e. Ensure materials from laboratory production/test/trial areas are placed in secure storage facilities outside working hours.

06304. Storage facility drawings. DE produces the standard drawings for storage facilities for MOD. The drawings take full account of these instructions. DE is to be consulted at the earliest stage when a new build or upgrade is

recommended. HOE are to ensure that any drawings or plans relating to their establishments storage facilities are retained and are available for inspection throughout the life of the building.

Storage of Weapons

06305. Man-portable weapons. When not in use all man-portable weapons, including mortars, are to be stored as follows:

a. **Complete weapons.** Complete weapons (include bolts/working parts) must be stored in secure armouries.

b. **Automatic weapons.** Automatic weapons, whether complete or not, must be stored in secure armouries.

c. **Personal weapons.** Personal weapons may be kept, when authorised by the HOE, in barrack rooms or place of work (e.g. offices), during working hours only but must be returned to armouries at the end of duty unless required for duty after normal working hours. HOE are to ensure that adequate security arrangements are made for personal weapons when they are not in establishment armouries.

d. **Pistols.** Pistols must be secured in secure armouries in one of the following ways:

(1) Behind an XPM 2089 screen or cage.

(2) In approved lockable steel cabinets.

(3) In bolt boxes bolted to the floor or wall of the armoury.

e. **Bolts.** Where non-automatic weapons have to be stored in a structurally approved (as opposed to secure) armoury, bolts must be removed from weapons to a separate building and stored separately. A bolt box, secured to the structure of the building as approved by the Principal Security Adviser (PSyA), would meet the requirement.

f. **Other small arms weapon parts.** The same degree of security as detailed in Sub-paragraph e above, must be provided for the following weapon parts and components:

(1) Barrels.

(2) Breech blocks.

(3) Firing pins.

(4) Springs.

(5) Magazines.

(6) Magazine housings.

g. **Large weapons.** Where the size of weapons precludes storage in armouries, Security Authorities are to issue specific instructions for their protection. Large weapons must, where possible, be stored in buildings, which, although not necessarily up to armoury standards, will afford a **Delay Time** which must be greater than the Guard Force's **Response Time**. When possible, firing needle assemblies and ranging devices must be removed and stored in secure armouries.

h. **66mm HEAT and LAW 80 rocket launchers.** All HEAT and LAW 80 rocket launcher tubes (including inert tubes) are to be treated as ACTO ammunition.

j. **Non-firing firearms.** Minimum security standards for non-firing firearms are as follows:

(1) **Innocuous.** To be protected to the same standard as live firing weapons.

(2) **Drill Purpose (DP) and Sectionalised Firearms (SI).** Where possible, DP and SI weapons should be stored in an armoury. Where this is not possible, they are to be stored in a mini armoury, approved arms chest or approved secure storeroom.

(3) **De-activated.** De-activated weapons are not required to be stored in an armoury. They are, as a minimum, to be stored in a robust, locked container if not displayed in a locked cabinet or securely mounted on a wall.

(4) **Imitation/Dummy.** Such firearms, which include replica weapons, are not to be stored in an armoury containing live firing weapons. They are, as a minimum, to be stored in a lockable container within a locked room.

k. **MILAN.** MILAN firing posts are to be protected to the same level as small arms and whenever possible stored in establishment armouries. Planning for new armouries should take account of this requirement. Where the use of existing armouries is impracticable they may be stored in a support weapons store or a building of comparable

security subject to local security advice. As for other natures, MILAN ammunition is to be stored separately from the firing posts.

l. **Sectionalised weapons.** Sectionalised weapons that expose the working parts can be reconverted to fire live rounds. Such weapons are to be held under secure conditions. These secure arrangements (which will vary according to location, number and type of stores, threat, etc) must meet security requirements laid down by PSyAs.

06306. Small Arms Trainers (SAT) weapons. SAT are to be held under secure conditions. These secure arrangements (which will vary according to location, number and type of stores, threat, etc) must meet security requirements laid down by PSyAs.

Storage of Protectively Marked Arms, Ammunition and Explosives

06307. Where protectively marked materials are to be stored, additional safeguards are to be considered. Policy given in this chapter and Chapter 5 should be employed to guard against both the terrorist and espionage threat.

06308. For the storage of SECRET or caveated material approved Type A security doors are to be used.

Explosive Materiel on Display

06309. Where explosive materiel is used for display purposes, all materiel must be:

a. Certified Free From Explosives (FFE) and clearly and indelibly marked as such (unless properly constructed and marked as Drill Purpose (DP) stores. In addition each item is to be marked with a unique local serial number that is recorded in a register.

b. When not in direct custody when being put to training use, all items are to be suitably secured in a locked display cabinet, room, building or compound appropriate to the highest Protective Marking applied to any of the items concerned.

c. If Protectively Marked CONFIDENTIAL or above, protected by an IDS and any other additional security measures required by the PSyA.

Note: Live materiel must never be used as training aids or for display purposes.

Weapons on Display

06310. Where weapons, including trophy weapons and bayonets etc, are used for display purposes, the following applies:

a. **Permanent display.** Only de-activated firearms may be permanently displayed, unless a dispensation for other weapons is authorised by Sector security staff. Weapons for display are to be:

(1) Certified as de-activated in accordance with Paragraph 06143 or as authorised by the PSyA.

(2) Firmly secured in a locked display cabinet and/or securely affixed to the fabric of the building.

(3) Provided with an alarm system where necessary.

b. **Temporary display.** Any non-firing firearm may be temporarily displayed when the weapon is:

(1) Made inert or inoperable by the removal of salient working parts.

(2) Locked or chained to the display stand and supervised at all times.

(3) Removed to secure storage when not supervised.

c. **Training aids.** Training aids must be supervised at all times when not secured as detailed in Paragraph 06206j.

06311. Before any room, building or area is brought into use to display items, for example in museums, at open days or on permanent display in instructional or crew rooms, permission and advice are first to be sought from the PSyA. Comprehensive orders are to be produced by the owner/custodian of the items and approved by the PSyA.

Weapons, Ammunition and Explosives in Laboratories, Test Chambers and Process Buildings

06312. Weapons are not to be left unattended in laboratories, test chambers or process buildings. ESyOs are to ensure that the storage of weapons meets the standards required in this chapter.

06313. Ammunition and explosives held in laboratories, test chambers and process buildings are to be protected within secure storage facilities that meet with explosive licensing requirements. Where this is not possible it may be

necessary for the ESyO or the Safety/Explosives Officer to ensure that suitable physical measures exist or arrange the removal of these items to suitably secure and licensed accommodation.

Arms Issued to Individuals

06314. Individuals are not permitted to keep Service arms or ammunition at home or in any private residence or accommodation accessible to the general public (e.g. hotels or clubs).

Security of Demountable Weaponry

06315. General. The security protection given to demountable weapons (as used on ships, vehicles or aircraft) is to be considered when the weapon is fitted and when the weapon is not. Due to the variety of different weapons and weapons systems that fall within this category, it is the responsibility of PSyAs to determine the specific security instructions for a demountable weapon. The standards applied to demountable weapons are not to be lower than the security standards for personal weapons.

Handling and Firing of MOD Weapons by Civilians

06316. The possession of MOD weapons by civilians is to be in accordance with current Firearms legislation, Armed Forces Act 1996 and MOD instructions including the requirement for security clearances. The term 'possession' covers the handling and/or firing of weapons and, for the purpose of this instruction, includes ammunition for those weapons.

06317. A civilian may be in possession of MOD weapons under the following conditions:

a. **Unsupervised**

(1) If the civilian is employed in the service of Her Majesty and in accordance with their duties as authorised by the HOE.

or

(2) If the civilian is under contract to the MOD and holds an appropriate and current Firearms Certificate or is covered by an appropriate and current Section 5 Authority issued by the Home Office under the provision of the Firearms Act 1968 where, in either case, such Authority is specific to the purpose of possession of MOD weapons on, in transit, or between,

Service property and in accordance with Service orders and regulations.

b. **Supervised.** On Service premises only, at events authorised by the HOE, such as open days, providing that each civilian is under supervision by a suitably qualified, competent and authorised member of the Armed Forces.

Storage of Privately Owned Firearms and Ammunition on MOD Property

06318. General principles. All privately owned firearms and ammunition must be the subject of a valid firearms certificate and must be stored in an approved Service armoury under regulations laid down for armouries or licensed explosive storehouses as appropriate.

06319. Storage on MOD property. If there is no Service armoury available, such arms and ammunition may be stored on MOD property provided that the following procedures are strictly adhered to:

a. Authority must be obtained from the HOE where the arms and ammunition are to be stored.

b. The civil police for the area in which the arms and ammunition are to be stored must be consulted under the terms of the Firearms Act 1968; their approval for the storage, and any security conditions that they may impose, must be obtained in writing; and such conditions must be complied with.

c. The approval of the PSyA is to be obtained. They may impose any further limitations above and beyond those required by a and b above.

d. On cadet force premises, only those private weapons needed to meet or supplement cadet forces training requirements are to be stored; no stored private weapon is to be of greater than .22 calibre, and handguns of all types are prohibited.

e. No type of firearm is to be owned by any individual unless he has a valid firearm or shotgun certificate.

f. Units owning full bore or small bore rifles or pistols for competition shooting purposes must comply with the Firearms Act 1968, Section 11. This necessitates the formation of a target-shooting club which must be approved by the Home Office.

g. Privately owned firearms and ammunition may be stored in establishment armouries and ammunition stores at the owner's risk, but only with permission of the HOE. They are to be accounted for and afforded the same security, including periodic checks, as Service arms or ammunition.

h. Privately owned firearms and ammunition are only to be used by the holder of the firearm certificate to which the firearms and ammunition relate.

06320. Long term safe custody. Personnel living in privately owned accommodation and posted overseas may request long term safe custody of privately owned weapons (but not ammunition) at a suitable establishment subject to the terms of this chapter.

Storage of MDP Owned Firearms and Ammunition

06321. Responsibility. The security of MDP weapons, ammunition and explosives is the subject of MDP regulations.

06322. Requests for storage. An MDP detachment, based at a MOD establishment, may request the establishment to provide safe custody of MDP weapons and ammunition if local circumstances are such as to prevent compliance with MDP regulations.

06323. Recording and checking. For purposes of recording and checking, MDP weapons are to be treated as Service weapons being held in safe custody.

06324. Issue. MDP weapons and ammunition are only to be issued on the authority of the Chief Constable, MDP or the HOE.

Security of Arms, Ammunition and Explosives during Range Practices and Exercises

06325. When arms, ammunition and explosives are taken out of armouries/storage for range courses and exercises, the security risk is greatly increased. In addition to a comprehensive security brief on the care, control and custody of arms, ammunition and explosives, the following precautions are also to be taken:

a. **Off-base range practices.** Standing orders are to be issued covering the procedure to be followed before leaving base and during the outward and return journey, and setting out the safeguards to be taken and checks to be made on arrival at the ranges, during firing practices, and before departure from the ranges. A complete check of all

arms and ammunition is to be made on arrival and on departure from the range and on return to the unit.

b. **Field exercises.** Responsibilities are to be clearly defined in standing orders for the safeguarding and carriage of arms, ammunition and explosives throughout the exercise. The following points should be included:

(1) Arms, ammunition and explosives are to be protected at all times. In camps and bivouacs where there is no secure armoury and ammunition store, arms, ammunition and explosives are to be centralized subject to safety rules under a 24 hour two person guard, or held in the care of the individual to whom they have been issued.

(2) When movement eventually takes place after a prolonged static period, a thorough 'sweep' of the areas vacated is to be carried out.

(3) A daily check is to be made of all personal weapons, ammunition and explosives held by individuals.

Note: Policy on movement of arms, ammunition and explosives is at Section II.

06326. Inert items of ammunition. Inert items of ammunition are to be afforded reasonable protection due to their potential for adaptation. A particular example of this danger is the tube of the 66mm HEAT or LAW 80 rocket launcher, which it is possible to convert after firing to launch illegally manufactured missiles. To guard against this risk, inert tubes are always to be handled and stored under secure arrangements. Tubes are to be accounted for and when no longer required they are to be returned to the appropriate ammunition depot.

06327. Accounting for ammunition and explosives on ranges and exercise areas. When live ammunition is fired it is to be accounted for directly on completion of the training period. All personnel are to be warned that the declaration that they are not in possession of live or blank rounds or empty cases, applies equally to explosives, pyrotechnics and accessories when used.

06328. Return of ammunition and explosives after exercises. Units returning from training are to ensure that ammunition and explosives are returned immediately to approved secure storage.

This page intentionally left blank

ANNEX A TO SECTION III TO CHAPTER 6

PHYSICAL SECURITY STANDARDS FOR ARMOURY BUILDINGS

General Physical Security Consideration and Siting

1. New armoury buildings are to be constructed in accordance with DE approved standard drawings. If there is a requirement for existing armouries to be rebuilt, approved standard drawings are to be used. Compliance with the regulations laid down in this Manual is not a justification by itself for the rebuild of existing armouries. where concerns about the standards of existing storage arrangements are raised, the advice of the PSyA is to be sought.

Doors

2. If possible, only one access door is to be used, which is to be kept locked when not in use. Detailed specifications for doors and door fastenings are:

a. All new building doors are to conform to approved standard drawings.

b. When fitted, the steel plate should be wrapped around the edges of the door and frame and secured on the edges and inside face by woodscrews, countersunk and spaced not more than 100mm apart. The metal faces are to be carried bolted at the centre and the corners, with the bolt heads fitted on the outside faces.

c. The frames on which the doors are hung should be of the same standard as the doors and should be securely fixed to the buildings by ragbolts at 600mm between centres, set to a depth of at least 50mm. If the building fabric is not suitable for ragbolts, the advice of Command security staff should be sought to determine a satisfactory method of securing the frame. Any gap between frame and masonry should be filled with material which cannot easily be removed.

d. Doors should open outwards and be hung on a minimum of three robust steel hinges which are to be capped and recessed.

e. A door security chain should be fitted and hinge bolts fixed to the frame and hanging edge of the door.

f. Doors are to be protected by an approved IDS.

3. If it is essential to fit double or sliding doors, padbolts must be fitted at the top and bottom of each section. Sliding doors should be fitted so as to slide internally. Sliding channels should be protected by fitting a raised concrete sill at floor level and a heavy metal retaining rail at the top, firmly fixed to the fabric of the building.

4. Ideally, where double and sliding doors are fitted, provision should be made for a small access door for personnel. The physical construction of this access door should be as specified in para 2: it is to be fitted with the locks and devices described below.

Locks

5. Two approved locks are to be fitted to armoury building doors (see Annex C). The types of locks to be used are:

a. Two rimlocks.

b. Two mortise locks

c. One rimlock and one mortise lock.

d. Dead locking 3 way multiple bolting system.

In general, new builds are to have locks included with the doorset, e.g. Benweld door with ASSA hookbolt deadlocks.

Windows and Ventilators

6. All non-essential apertures are to be bricked up. Remaining windows are to be of the non-opening type and are to be located as high above ground level as possible. They are to be constructed or protected as follows:

a. Windows should be made either of wire reinforced translucent glass, or of glass bricks to SSG Outline Specification No 8 set in concrete or a steel frame. The frame should be an integral part of the building so that it cannot be easily removed.

b. Window bars should be constructed as per SSG Drawings PS 301 or PS 302. The bars are, however, at 150mm centres with 45 x 6mm rails at 200mm centres in 50 x 50 x 6mm angle frame, bolted/screwed to the wall. (SSG specification No 8 blocks do not require bars).

c. Windows are to be included in the IDS.

d. If the local security situation warrants additional security, e.g. to prevent explosive or toxic devices from being introduced into the buildings, the window should be covered by sheets of heavy gauge mesh welded to a metal frame and bolted to the masonry.

7. Where the fabric of the building will not permit steel bars to be secured into position, they should be welded to a frame of similar metal which should be welded or burred to prevent their removal. The framework is to be securely bolted through the building fabric.

8. If ventilators are necessary, they should be of the staggered airbrick variety and must be as strong as the rest of the building. If not, they are to be reinforced with heavy gauge mesh. If the interior of the building can be viewed through the ventilator, with or without the interior lights being switched on, the ventilator is to be covered with metal sheeting, standing proud from the ventilator to permit air circulation. The metal sheeting should be of sufficient strength to prevent easy bending or distortion and should be so fixed to the fabric as to prevent unauthorized removal from the outside. Consideration should be given to fitting offset ventilators.

9. If a fan or trunk ventilation system is necessary, care must be taken to ensure that all inlets and outlets are fully protected. Any suitable method described in the preceding paragraphs may be considered. Additionally, a heavy narrow gauge XPM sheet, welded or brazed on to a frame and securely bolted into position in the trunking, may be used.

Hatchways

10. Where a hatch is necessary, e.g. to facilitate the issue of arms it should be protected by whichever of the methods described above is most suitable. The hatchway is to be included in the IDS and should incorporate identification slots and sentry door viewers.

Intruder Detection Systems

11. A Class 4 IDS (see the Catalogue of Security Equipment for details) is to be installed in all armouries containing weapons classified as ACTO as listed in Chapter 6 para 06104b and those weapons considered by Service Security Authorities to require such protection. The purpose of the IDS is to ensure that the response force can respond in accordance with para 06130 or 06131.

12. The IDS is to provide an audible alarm as a deterrent to an unauthorised entry and an alarm signal to an alarm panel located in a 24 hour manned secure control centre.

13. A manual emergency alarm system, consisting of a duress alarm, is to be installed within the armoury so that the occupants can raise the alarm in the event of an attack. This alarm is to be located near doors and issue hatches and should sound an audible warning as a deterrent, and provide an alarm signal to a warning panel in a 24 hour manned secure control centre.

14. The advice of the PSyA is to be sought on the type of IDS and alarm system to be installed.

15. System activating keys are to be treated as security keys and safeguarded in accordance with the instructions in Chapter 5.

Inspection Grilles

16. A sentry door viewer should be fitted to external doors and issue hatchways to permit the positive identification of persons seeking entry. An inspection grille, suitably protected and large enough for identification documents to be passed through for scrutiny, should also be let into the doors of buildings where control of entry is in force, and into issue hatchways.

Internal Doors

17. Internal doors of armoury buildings, which directly lead to weapons, should be constructed to the same standard as external doors, as per para 2.

Security of Weapons

18. Weapons are to be stored so that they cannot be removed quickly or easily by a person who has gained unauthorized access to the armoury building. This can be achieved in a number of ways depending on the type of weapon to be protected. 'In use' weapons can be stored on a rack or in a steel cupboard and secured with a high tensile steel rod or bar or a suitable steel wire rope, spliced and bound with copper wire and then soldered or mechanically joined by the Talurit method, passed through the rack or cupboard and the trigger guards of the weapons. The rod, bar or wire is then fixed by 2 hasps and secured by a security padlock. The fixing bolts of the hasps should be properly secured, preferably by being secured into the building structure. Racks and storage cupboards should be securely bolted to the floor and fabric of the room.

SA80 Weapon Racks

19. SA80s are to be stowed in specific purpose built racks. Chessington drawings 16 40 007 and 16 40 098 refer.

Security Lighting

20. The provision of external lighting for armoury buildings must take account of the need to create a high degree of illumination and eliminate shadows. A lighting factor of 3.0 lumens per 900 square centimetres should be achieved to illuminate the building and its immediate surroundings. Lighting fixed to armoury buildings should be in sealed glass bulkheads, located above the entrance doors and at all corners at a height of between 2.44m and 3.05m. The operating switches for this lighting should be located either within the building or in a secure position.

Security Keys

21. External keys to armoury buildings and keys to internal weapons stores are to be protected in accordance with Chapter 5, i.e. as security keys. Keys to internal weapons stores are not to be secured within the armoury building and are to be kept separate from the external door keys. The security of keys is to be so arranged so that one person cannot gain access to both arms and ammunition.

This page intentionally left blank

ANNEX B TO SECTION III TO CHAPTER 6

MINIMUM PHYSICAL SECURITY STANDARDS FOR BUILDINGS CONTAINING ACTO EXPLOSIVE STORES

1. Buildings containing ammunition and explosives are to be constructed according to the standards set by the Explosives Storage and Transport Committee (ESTC), which are incorporated into the mandatory Service explosive regulations. A representative of the CIE will assist in the selection of the building type to be considered and provide guidance to the designer on the service regulations to be applied. These standards and regulations shall be read in conjunction with DE (Specialist Construction Group) (DE(SCG)) Works Services Functional Standards. DE(SCG), as the Works Technical Authority for physical security and explosive buildings, should be consulted for design approval prior to construction.

2. For security reasons the following principles and design requirements are to be applied to all new buildings, and as far as is practicable, when improving existing facilities to a commensurate standard, to store ACTO explosive stores.

General Physical Security Consideration and Siting

3. Explosives buildings should not be sited in remote areas unless a satisfactory combination of security patrols, response forces, intruder detection system (IDS) and local orders ensure the physical security of the explosives.

4. The ESTC design standards cover a variety of construction options including reinforced concrete, earth covered igloo structures, free standing, traversed, brick structures and light frangible buildings each with the minimum of openings that require security safeguarding. Where new or conversion work is being considered, DE(SCG), the PSyA and the CIE advisor will highlight any short-comings in the design that could be a potential security risk; these short-comings are to be addressed during the design phase and eliminated as far as is practicable. The following specific design requirements for components of the building are to be considered during the design phase and incorporated as necessary.

Frangible Blow-out Panels

5. Some approved designs of explosive buildings incorporate blow-out panels, which are provided to fail in the event of an internal explosive event. These blow-out panels are not as strong as the remainder of the structure and depending on their design may require additional security devices to prevent access, without inhibiting design failure, from the outside of the building. When all explosives are removed from the building at cease work the additional security requirements may be permanently waived.

6. A blow-out panel of brick, concrete or similar construction (unsuitable for HD1.1 containment structures) will not appear different from the remainder of the building and no further security devices will normally be necessary, although it must not be obstructed in any way. When security considerations are to prevent the introduction of explosive or toxic devices into the building through the blow-out panel, then a solid blow-out panel of this type is generally used.

7. A frangible blow-out panel made from glass, glass reinforced plastic or similar (suitable for HD1.1 containment structures) will need to be safeguarded by the fitting of bars. These bars may be incorporated into the blow-out panel itself but must be positioned internally so as to permit unrestrained venting. When bars are used they are to conform, as a minimum, to the diameter and spacing, and/or fixing specified at para 12b or 13.

Doors

8. Doors used on explosive buildings are specified by the ESTC and may override the security requirements because explosive safety considerations specify a particular type and construction. The construction of the doors to meet the minimum security requirements is detailed below and is to be applied if the ESTC guidelines are not specific:

a. If possible only one access door is to be used.

b. All doors are to be kept locked when the building is not in use.

c. For all new buildings doors are to conform to the Government standard "Chessington" Drawing No DW 55713/3 Sheets 1 - 16.

d. For existing buildings being modified as explosive buildings the doors are to be of minimum 44mm thick solid hardwood core construction, covered by 1.6mm mild steel on both sides and edges, and fitted with hinge bolts. The steel plate is to be secured on all edges and the inside face by woodscrews, countersunk and spaced not more than

100mm apart. The metal faces are to be carriage bolted at the centre and corners, with the bolt heads fitted from the outside face.

e. The frames upon which the doors are hung should be of the same standard as the doors. The frame should be secured to the building by a suitable secure bolt system at 600mm centres, with a minimum embedded length of 100mm. Any gap between the frame and masonry should be filled with a fireproof and tenacious mastic.

f. Doors should normally open outwards, except when the building design requires inwardly opening doors for the containment of an explosive event, and be hung on a minimum of 3 robust steel hinges, which are to be capped and recessed.

g. Doors are to be protected by an IDS approved by the appropriate PSyA and the CIE.

9. When double or sliding doors are specified, padbolts must be fitted internally at the top and bottom of each section. If sliding doors are specified they should be fitted to slide internally if possible. Sliding channels should, if operating conditions permit, be protected by fitting a raised concrete sill at floor level and a heavy metal retaining rail at the top which is securely fixed to the building fabric.

10. Ideally a personnel access door should be fitted when sliding or double door sets are specified. The physical characteristics of this type of door are to be the same as specified in this Annex.

Locks

11. Locks from the approved types listed at Annex C are to be fitted to explosives building doors. The number and types of locks to be fitted to buildings storing explosives are to be selected from the following:

a. Two rimlocks.

b. Two mortise locks.

c. One rimlock and one mortise lock.

d. Two dead locking 3 way multiple bolt system.

Windows and Ventilators

12. All non-essential apertures are to be bricked up. Apertures required for ventilation of the building contents or venting (blow-out panels) shall not be

obstructed. Essential windows are to be of the non-opening type and located as high above ground level as possible. They are to be constructed or protected as follows:

a. Windows are to be made from laminated glass or glass bricks set either in concrete or a steel frame that is integral with the building and not easily removable.

b. High tensile steel bars are to be fitted. They are to be not less than 20mm in diameter, spaced apart not more than 125mm between centres, and set into the fabric of the building. The bars should be held in place by 40 x 10mm flat steel spacers or plate spaced at not more than 460mm. The spacers should have 'T' ends that are secured to the fabric with cement grout to a depth of 150mm on either side of the window.

c. If windows are fitted they are to be protected by detectors connected to the IDS.

d. If additional security warrants, e.g. to prevent the introduction of explosive or toxic devices into the building through the windows, then sheets of heavy gauge welded mesh shall be welded to the window frame.

13. Where the fabric will not permit steel bars to be secured into position, they should be fixed internally by welding to the frame.

14. If ventilators are specified they should generally be air-bricks and of equivalent strength as the rest of the walling. If this cannot be achieved they are to be reinforced with heavy gauge expanded metal sheet fixed to the interior of the building in such a way as to prevent unauthorised removal.

15. If a fan assisted ducted ventilation system is specified care must be taken to ensure all inlets and outlets are protected. Bars or narrow gauge XPM sheet shall be provided within the ductwork at the security boundary. This must be welded or brazed to a frame and securely bolted into the ducting.

Hatchways

16. Where a hatch is necessary, i.e. to facilitate the issue of stores, it should be protected by whichever of the methods described in this Annex is most appropriate. The hatchway is to be included in the IDS.

Intruder Detection Systems

17. A Class 4 IDS is to be installed in all buildings used for the long term storage of ACTO ammunition and explosives listed or associated with, the

weapons in Chapter 6, para 06104b and those ammunition and explosives considered by the Security Authority to require such protection. The purpose of the IDS is to ensure that the response force can respond in accordance with para 06131 or 06132.

18. An exception to para 17 may be granted by the PSyA for short term storage, following consultation with the CIE and where an appropriate guard, patrol or alternative security device or measure is provided so as to respond to any unauthorised entry in time to prevent the loss of or damage to the ammunition and/or explosives being protected.

19. An IDS is to provide an audible warning as a deterrent to an unauthorised entry and an alarm signal to an alarm panel located in a 24 hour manned secure control centre.

20. A manual emergency alarm system, consisting of a duress alarm, may also be provided within the building so that the occupants can raise the alarm in the event of an attack. Such an alarm is to be located near doors and issue hatches and should sound an audible warning as a deterrent, and provide an alarm signal to a warning panel in a 24 hour manned secure control centre.

21. The advice of CIE, DE(Works) and the PSyA is to be sought on the type of IDS and alarm to be installed. Any IDS or alarm must electrically meet the requirements of the electrical category of the explosives building.

22. System activation keys are to be treated as security keys and safeguarded in accordance with the instructions in Chapter 5.

Inspection Viewers and Grilles

23. A sentry door viewer is to be fitted to external doors on guardrooms where explosives are stored to permit identification of persons seeking entry. A viewer is not required on those explosives buildings that are used solely as storehouses and process buildings. An inspection grille should be fitted into the door of buildings where control of entry is in force. The grille should be large enough to permit identity documents to pass through it.

Internal Doors

24. Internal doors protecting the explosives being stored are to be of the same or equivalent standard as the external door type specified in para 8d. Alternative equivalent doors may be found in JSP 411. For example the secure gas-tight door at Figure 22 would be suitable.

Internal Storage

25. Where explosive safety regulations permit explosives to be stored in manned areas the explosives are to be stored in authorised storage devices. Keys to internal explosive stores are not to be secured within the building containing the internal store, but are to be kept separate from the external keys in a secure place and safeguarded in accordance with the instructions in Chapter 5.

Security Lighting

26. The provision of external lighting for explosives buildings must take account of the need to create a high degree of illumination and eliminate shadows. This requirement must be balanced against the overriding safety requirement when the building is on an airfield.

27. A level of illumination of 4 LUX should be used to illuminate the buildings and surrounding area. When the luminaire are mounted upon columns they are to be positioned such that there is a distance of one and one-half times the height of the stanchion from the building to the luminaire. Luminaires fixed to buildings are to comply with the ESTC standards and service regulations for electrical equipment used in explosives areas, and mounted at the corners of the building at a height of between 2.5 and 3.0m. Lamps in sealed glass bulkheads may be mounted above the doors of the building to illuminate the area in front of the doors. Operating switches for security lighting should be located in a secure cabinet attached to the external wall of the building or operated automatically.

Fences

28. Consideration should be given to providing a security fence if the local situation dictates the need. The PSyA is to be consulted on the need for, and (if required) standard of the fence. When a security fence is required the fence should be positioned at least 20m from any explosives storage building. The keys for the access gates are to be treated as security keys and handled in accordance with the instructions in Chapter 5.

Other Security Criteria

29. The instructions for security patrols, response forces and security orders detailed in this chapter apply. In addition the protection of security keys is to be in accordance with the instructions in Chapter 5.

ANNEX C TO SECTION III TO CHAPTER 6

APPROVED LOCKS AND DEVICES FOR ARMOURY BUILDINGS

Rimlocks

1. The Avon Locking Unit is the only rim lock suitable for armoury use. The following locks remain suitable for armoury use but are not to be used for new constructions and replacements of unserviceable locks unless an Avon Locking Unit cannot be physically fitted:

a. The Avon Rim Fixed Deadlock.

b. Ingersoll SC71.

c. Ingersoll SC73.

d. Ingersoll D20.

Mortise Locks

2. The locks listed below are the only mortise locks suitable for armoury use:

a. Chubb 3R35 locking latch.

b. Chubb hookbolt 3M50.

c. Chubb 3K70(upright).

d. Chubb 3J60 (horizontal).

e. Chubb 3G110.

f. ASSA Twin 6000 with 9788 high security deadlock.

Note: Hookbolts must always be used for double and sliding doors.

Hinge Bolts

3. Security hinge bolts - e.g. Chubb pattern WS7.

Door Security Chains

4. Doormaster security door chain - Chubb pattern WS6.

Sentry Door Viewer

5. Door viewer - Chubb pattern WS8. This provides a 175° angle of vision and only permits viewing one way.

SECTION IV

SECURITY OF CADET FORCES ARMS AND AMMUNITION

Introduction

06401. The general principles given in this section are to be applied to the storage of cadet forces' arms and ammunition. The movement of cadet forces arms and ammunition (e.g. from cadet forces to ranges and shooting camps) is to be in accordance with Section II of this chapter. Whenever possible, arms and ammunition are to be stored in Service establishments; the regulations for storage on regular establishments are contained in Section III. However, alternative storage facilities may need to be authorized and the Matrix for the storage of arms and ammunition within cadet force premises described at para 06190, has been so designed to identify the criteria required for storage in these circumstances.

Security of arms and ammunition - General principles

06402. Under normal circumstances all Service-owned arms and ammunition are to be stored in an approved armoury/storeroom. An approved armoury/storeroom is:

a. A Regular Service armoury.

b. A Reserve forces armoury.

c. A Home Office armoury, if previously approved by the appropriate single-Service Security Unit.

d. A mini armoury or approved arms chest.

e. A secure storeroom, in accordance with Section III.

Dispensations for cadet forces

06403. **Permanent storage.** Where there is no approved armoury within a reasonable distance of the cadet force unit, permanent storage will be considered if the premises meet the criteria detailed in the matrix at Annex A.

06404. **Temporary storage.** Service-owned arms and ammunition may be temporarily stored (up to 48 hours) in cadet force premises that do not meet the

standards of sub paras d or e above, where the facilities meet the index for short term storage detailed in Annex A.

06405. **Transport of cadet weapons**. In general, up to 2 Service-owned weapons and where necessary up to 1000 rounds of rimfire ammunition may be transported in a private vehicle by an adult member of the cadet forces' uniform cadre. Quantities may be varied in accordance with single-Service instructions. All other provisions of Section II, regarding the precautions to be taken during transit, apply. (Particular attention is drawn to sub-para 06062.c above).

Matrix for the storage of arms & ammunition within cadet forces premises.

06406. **Methodology.** The matrix at Annex A is to be used for the storage of arms and ammunition within cadet force premises. It is similar in methodology to the Minimum Baseline Measures Matrix used in Chapter 5 for physical security. A set of baseline scores has to be met in order for arms and ammunition to be stored on cadet force premises. The standards required are divided into 4 categories as follows:

a. Permanent Storage.

b. Temporary Storage.

c. Emergency Storage.

d. Storage of DP Weapons.

06407. **Security standards matrix.** The security standards matrix is at Annex A. It details the scores required for the 4 categories for both high and low risk areas.

06408. **Storage indices.** The indices used to calculate the score for use with the Matrix is at Annex B.

Withdrawal of weapons & ammunition

06409. Heads of establishments or their nominated deputies, are to give written authority on every occasion that centre-fire/full bore weapons and ammunition are drawn. The weapons and ammunition are to be returned to authorized premises immediately following use.

Certificate of security for armouries

06410. **Initial certification**. All cadet force armouries holding arms and ammunition are to be subjected to an initial survey by the appropriate single-Service security unit

before being certified to hold arms and ammunition. Certification, is only to be given following the implementation of essential recommendations.

06411. **Issue of certificate**. Arms and ammunition are not to be stored on premises until the security unit has given approval and the appropriate cadet force HQ has issued a certificate of authority to hold arms and ammunition.

06412. **Location of certificates.** The certificate is to be retained with the arms register and a duplicate retained by the appropriate HQ.

06413. **Security unit reports.** Security unit reports, following inspections, or security investigations, are to be forwarded to the appropriate Cadet Force HQ and PSyA, with recommendations for the improvement of security facilities. The HQ is to define those recommendations essential for the security of unit arms and direct the unit to implement the modifications. The HQ is to decide, with the advice provided by the security unit whether to withdraw temporarily the authority to hold arms pending the implementation of the recommendations. When unit authority is withdrawn, the arms and ammunition are to be removed immediately and stored in an authorized armoury.

Inspections of armouries by security units

06414. In addition to the initial survey of a cadet force's armoury, inspections by security units are to be undertaken in the following circumstances:

a. When any doubt exists whether the cadet force unit's security standards are adequate to safeguard its arms and ammunition eg following a break-in.

b. Periodically, as prescribed by the appropriate PSyA to ensure appropriate security standards are being maintained.

Inspections by cadet force HQs

06415. Cadet force unit security procedures and arms are to be checked periodically by HQ staff at intervals of not more than 12 months. Periodically, a check is to be made without prior notice. When visiting units, regional staffs are to check that security standards are being maintained.

Registers

06416. Cadet forces are to maintain 3 registers:

a. **Small Arms Register**. This register is to bear the serial number of the weapons on charge and the dates of voucher and receipt numbers.

b. **Check of arms register**. This register is to be maintained as follows:

(1) All weapons held within the cadet force premises are to be listed individually by type.

(2) Arms and ammunition are to be checked by an adult member of the cadet force on every occasion that the unit is open. Each check is to be recorded in the register, which is to be signed and dated by the checker.

(3) The register is to contain the certificate of authority to retain arms and ammunition on the premises.

(4) The register is to be signed by any officers making periodic security inspections.

c. **Safe Custody Register**. This register is to contain details of weapons held in safe custody (e.g. for other cadet force units).

Keys

06417. **Protection of keys**. Keys are to be protected as follows:

a. **Armoury keys.** When the armoury is not being used to receive or issue arms and ammunition, the armoury door is to be locked. The keys are to be held on a dedicated separate key ring held by the unit commander or his deputy.

b. **Approved arms chest keys.** When not being used to receive or issue arms, arms chests are to be locked. The keys held on a dedicated separate key ring by the unit commander or his deputy.

c. **Ammunition boxes.** When not being used to receive or issue ammunition, ammunition boxes (see para 06214) are to be locked. The keys are to be held on a dedicated separate key ring held by the unit commander or his deputy. (Where possible the ammunition box keys are to be held by a separate person).

d. **Other security keys.** Other unit security keys are to be kept in the possession of the unit commander or an adult member of staff on a separate key ring to those listed in sub-paras a to c above.

e. **Duplicate keys.** The duplicate keys to those listed in sub-paras a to d above are to be deposited in accordance with single-Service Instructions.

06418. **Orders**. Orders regarding the custody and issue of keys are to be promulgated by the unit commander. They are to be regularly reviewed.

Liaison between cadet force units and the civil police

06419. Personal liaison between officers commanding cadet force units and the local police authorities is essential. The police may agree to routine patrols of cadet force buildings where rifles are held, or accept rifles, bolts and magazines and ammunition for short-term custody following unauthorized entry to the premises.

Alarm system

06420. Units are encouraged to install a suitable alarm system. Appropriate HQs are to consider fitting an alarm system at those units where the civil police advise that it is essential. Alternatively HQs are to order the removal of the arms and ammunition to a secure authorized armoury.

Private weapons

06421. The cadet forces do not accept financial responsibility for any private weapons placed in safe custody with Service issued weapons. The term 'private weapons' includes weapons owned by private individuals and those purchased by the unit concerned. The regulations concerning the handling, storage, safe custody and disposal of these weapons are contained in the Firearms Act 1968. This Act also requires that, when private weapons are held on unit premises, a firearms certificate is required.

06422. In order to qualify for a free issue of a firearms certificate, units require the approval of the Secretary of State. Applications for such approval should be made to the Home Office through local police stations or the National Rifle Association or National Small-bore Rifle Association. Applications should give the correct title of the unit, the type and calibre of weapons concerned, the range or ranges used, and the home address of a responsible adult to whom the firearms certificate can be issued.

06423. Only those private weapons needed to meet or supplement cadet force training requirements are to be stored in a unit's armoury/arms chest. No stored weapon is to be greater than .22 calibre. Handguns of all types are prohibited.

06429. *Spare.*

Losses and recoveries of firearms

06430. All losses and recoveries of firearms and ammunition are to be reported in accordance with the format in Section I.

Physical security of cadet force secure storerooms

06431. Purpose-built storerooms for cadet forces are to comply with the following structural standards:

a. External walls of the building are to be of 275 mm cavity brick, concrete block or stone, and internal walls of the armoury are to be of 225 mm solid brick, concrete block or stone.

b. Floors and roofs of armoury rooms are to be of 150 mm concrete.

c. Windows trapdoors, fanlights, etc. are not to be incorporated in the armoury rooms.

d. There is to be only one access door to the armoury room, which is to be to the standard laid down in Annex A to Section III:

(1) All new buildings doors are to conform to SSG Chessington Drawing No DW 55713/3 sheets 1 - 16. For existing buildings, doors should be of solid core construction at least 40 mm thick covered by 1.6 mm mild steel on both sides and fitted with hinge bolts.

(2) When fitted, the steel plate is to be wrapped around the edges of the door and frame and secured on the edges and inside face by woodscrews, countersunk and spaced not more than 100 mm apart. The metal faces are to be carriage bolted at the centre and the corners, with the bolt heads fitted on the outside faces.

(3) The frames on which the doors are hung are to be of the same standard as the doors and should be securely fixed to the building by ragbolts at 600 mm between centres, set to a depth of at least 50 mm. If the building fabric is not suitable for ragbolts, the advice of PSyAs should be sought to determine a satisfactory method of securing the frame. Any gap between frame and masonry should be filled with material which cannot easily be removed.

(4) Doors are to open outwards and must be hung on a minimum of 3 robust steel hinges which are to be capped and recessed.

e. Approved locks of the type listed in Section III, Annex C, are to be fitted to armoury buildings doors. The types of locks to be used are:

(1) Two rimlocks.

(2) One rimlock and one mortise lock.

(3) Two mortise locks.

(4) Two padlocks with heavy duty padlock bars.

06432. **Modernisation or upgrading of existing buildings.** When existing buildings are modernized or upgraded, they are as far as practicable to incorporate the specifications above. Examples of improvements are given below:

a. **Walls, ceilings and floors.** Weldmesh or heavy gauge expanded metal sheeting may be fixed to the walls, ceilings and floors to improve the protection of soft skinned (e.g. Spooner or modular type buildings) and inferior internal walls and ceilings.

b. **Windows.** Any of the following may be considered for reinforcing windows, ventilators, trapdoors and fanlights:

(1) **Glass bricks.** Glass bricks in pre-cast panels, i.e. bricks pre-set into a concrete honeycomb rather than built in singly as in a brick wall.

(2) **Steel roller shutters.** Where steel roller shutters are used, it is important to ensure that the guide frames are firmly secured to the side walls and the locking mechanism is as strong as the shutter.

(3) **Steel shutters (casement type) on the outside of windows.** It is important steel shutters (casement type) are capable of being secured from the inside.

(4) **Gates.** Gates are to be secured by an approved lock. The gates are to be fixed in a position with expanding bolts or bolts cemented into the masonry or brickwork; woodscrews and plugs are not to be used.

(5) **High tensile steel bars.** Steel bars not less than 19 mm in diameter and at not more than 127 mm centres, held in place by flat steel spacers at not more than 457 mm intervals. The spacers are not to be less than 38mm x 10mm and be secured into the masonry or brickwork.

(6) **Expanded metal or weldmesh.** Heavy gauge expanded metal or weldmesh welded to a metal frame and bolted to the masonry.

c. **Doors.** Ideally approved, purpose built, security doors and furniture are to be used. However, wooden doors of solid laminated hardwood core or solid multi-ply construction not less than 54 mm thick may be used and can be improved as follows:

(1) By facing or backing with mild steel sheet.

(2) Fitting dogbolts and approved locks and bolts.

(3) Mortise locks backed with mild steel sheet.

(4) Fitting mild steel angles to wooden doorposts, and improving the fixings between wall and frame. Additional heavy duty hinges may be required to support the increased weight.

06433. The advice of the appropriate PSyA and the appropriate security unit is to be sought before implementing enhanced security measures.

Security of weapons

06434. Only .22 (rimfire) calibre weapons, DP and sectioned weapons not falling into the category laid down in para 06004b, are to be stored in cadet force premises. The security requirements are:

a. Storage is to be in an approved mini armoury or in Benweld/Thompson/Kennedy arms chests located in the unit storeroom. The weapons are to be secured through the trigger guards by steel chains or steel cables and padlocks with the chains/cables welded to the side walls. The outline specification for the mini armoury is contained at para 06217.

b. The approved arms chests are to be secured by ragbolts through the base into the solid building foundations with the opening edge next to a wall to prevent leverage. A concrete infill or plinth is required for buildings on stilts which permit access to the underside of the building.

c. Additionally, Thompson arms chests are to have:

(1) Two approved mortise locks.

(2) Two approved model security hinge bolts fitted on the hinged edge of the door/lid.

(3) The door outer edge modified at source with integral lip; or angle iron fitted top to bottom, tack welded - weld spots at intervals down full length of outer edge; or angle iron fitted from top to bottom with a continuous or running full length weld; or angle iron fitted from top to bottom, tack welded - with the 2 areas covering the lock tongues continuous welded over a length of 60 to 75 mm.

(4) Steel chains or cables with padlocks fitted. The cables are to be located in, and welded to, the side walls of the arms chest.

Security of ammunition

06435. Under no circumstances is ammunition greater than .22 calibre to be held on cadet force premises. Storage of .22 ammunition is to be in one of the following:

a. An approved mini armoury.

b. Security lockable approved ammunition boxes located in the armoury and ragbolted into the floor or other substantial feature of the building structure in such a manner that level access is prevent (eg opening edge to a wall) by:

(1) Ragbolting onto the arms chest plinth.

(2) Bolting to the top of the arms chest plinth.

(3) Ragbolting into the floor or other substantial feature of the building structure.

c. Ex-MOD cash safes.

d. A lockable steel container secured to the inside of a further steel container (pending the issue of approved ammunition boxes).

06436. **Ammunition stocks**. Stocks of .22 ammunition are to be kept to the minimum compatible with training requirements. A maximum of 2000 rounds may be held at the unit in approved ammunition boxes or ex-MOD safes and up to 5000 rounds in an approved mini armoury. Where a unit wishes to hold more than 10000 rounds for geographic distribution purposes, their security facility is to be inspected for suitability by the appropriate security unit. A storage limit compatible with the secure facility will be approved. All issues and receipts are to be entered in an ammunition issue/receipt log.

Security of rifle bolts and other weapon parts

06437. Unless the cadet force armoury is a secure or structurally approved armoury, rifle bolts for weapons of greater than .22 calibre are not to be stored in cadet force premises. When not in secure or structurally approved armouries, bolts for .22 rimfire and DP weapons are to be removed when not in use and stored in robust steel arms chests, ex-MOD cash safes, or lockable steel bolt boxes of robust construction firmly secured to the structure of the secure room. Other weapon parts such as barrels, breech blocks, firing pins and magazines may be stored with the bolts. The storage containers holding bolts and weapon parts are not to contain ammunition, which is to be stored separately in a secure container or purpose built arms chest.

Mini-armouries

06438. Mini-armouries have the following significant features:

a. The floor and roof are to be 150 mm reinforced concrete.

b. Walls are to be 215 mm solid brick (engineering brick), concrete or stone.(1)

c. Straight ventilators protected on the outside by a steel plate rag bolted at the corners and the bolt heads spot welded are to be installed.

d. There are to be 2 separate compartments, one for arms and one for ammunition, divided by a 6 mm steel plate built into brickwork at front and sides and welded to front angle iron.

e. Each compartment is to have a steel security door hung on 3 robust steel hinges not less than 60 mm which are to be capped and recessed.

f. Each door is to be fitted with 2 Chubb 3M50 locks.

Note:

(1). Facilities built before Jul 92 having walls constructed of 275 mm cavity brickwork with stepped ventilators are acceptable.

ANNEX A TO SECTION IV TO CHAPTER 6

SECURITY STANDARDS AT CADET FORCES PREMISES

The following matrix should be used to calculate the minimum security index required to permit the storage of Service- owned weapons and ammunition on cadet forces premises. Once the required index is known, use the tables at Annex B to calculate the index value of security features present. Using Annex B the index for a given Unit can be calculated and compared with the minimum requirement. If there is a shortfall then Annex B can be used to determine the security enhancements that could be made to bring the premises up to standard.

Serial No	**Purpose**	**Risk level**(1)	
		High Risk	**Low risk**
(a)	**(b)**	**(c)**	**(d)**
1	Permanent storage	33	25
2	Temporary storage	25	20
3	Emergency storage (<24 hours)(2)	20	15
4	Storage of DP weapons	20	15

Notes:

(1) The risk is determined by the appropriate single-Service security unit and is based upon a civil police assessment of the burglaries in the area, the amount of any other arms, ammunition and explosive items within the unit and any other factors relevant to individual locations. Where a security unit has not carried out on assessment, the risk level is to be based on the insurance risk assessment used by national firms.

(2) Emergency storage in substandard premises may only be undertaken in exceptional circumstances, when weapons normally lodged elsewhere cannot be returned to their parent armoury that day.

ANNEX B TO SECTION IV TO CHAPTER 6

INDICES FOR THE STORAGE OF ARMS AND AMMUNITION WITHIN CADET FORCES PREMISES

1. To determine the security index of a cadet force unit:

a. For each of the 3 sections below examine the measures or facilities that are in place and note the score for each.

b. Add the scores together for the section total.

c. Add the section scores together for the total index. (The total index must include a score from each section).

Section One

Containers (use para 2 or 3 for weapons and ammunition respectively)

1. Armouries.

a.	Regular Service or TA.(1)	NA
b.	Home Office.(2)	35
c.	Mini armoury.(3)	30

Either:

2. Arms Chests.

a.	Benweld.(4)	25
b.	Benweld.(5)	15
c.	TAC.(4)	10
d.	Kennedy.(4)	10

Or

3. Ammunition Containers

a.	H-60 Box (ammunition or bolts only).(4)	10
b.	Other ammo boxes detailed at para 06214.(4)	10

Section one score:

Notes:

(1) If weapons are stored in a Regular Service or Reserve Forces, armoury no further action is required.

(2) Subject to prior approval by the appropriate single-Service security unit.

(3) Mini armouries are not considered stand-alone items. Therefore other sections in this matrix apply also to establishments which hold mini armouries.

(4) Installed in accordance with JSP 440, Chapter 6, para 06213(b).

(5) Not installed in accordance with JSP 440, Chapter 6, para 06213(b).

Section Two

Storeroom (housing the Arms Chest/Ammunition Container)

1.	**Secure storeroom**[6].		25 (go to Section 3)
2.	**Walls**. Each wall scored individually.		
	a.	Double brick/stone/concrete block.	4 each
	b.	Reinforced concrete.	4 each
	c.	Single brick/stone/concrete block.	3 each
	d.	Wood or other robust material (include Portacabin/Spooner Hut wall).	2 each
	e.	Plasterboard or similar (internal wall only).	0 each
	f.	XPM or Weldmesh lined.	add 2 each wall for each layer of (separated) XPM[7]
			Sub total:
3.	**Floor & Ceiling**. A single score for the weakest part of the floor or ceiling of the room housing the Arms Chest/Ammunition Container.		
	a.	Concrete.	2
	b.	Wood/Ply.	1
	c.	Plasterboard.	0
	d.	Ceiling tiles.	-1
	e.	XPM or Weldmesh lined.	add 2 for each layer of (separated) XPM[7]
			Sub total:
4.	**Securing point of Arms Chest**		
	a.	Concrete plinth or concrete floor.	2
	b.	Other.	0
			Sub total:

5. **Windows**. A score based upon the weakest window in an external wall of the room housing the Arms Chest/Ammunition Container.

a. Protection.

(1)	No window.	Add same index as the wall from 2 above
(2)	Bars/metal shutters/glass bricks/XPM.[8]	2
(3)	Sealed or lockable.[9]	1

b. Frame

(1)	Metal or PVCu frames.	1
(2)	Wooden frames in good order.[10]	0
(3)	Wooden frames in poor order.[11]	-1

Sub total (a+b): (Max index of 4)

6. **Door**. A single score for the weakest of any internal door affording access to the storeroom housing the Arms Chest/Ammunition Box.

a.	(1)	Steel door.[12]	3
	(2)	Steel faced door.[12]	3
	(3)	Modified wooden door.[13]	2
	(4)	Wooden fire door (half-hour resistance).	1
b.		Door opening outwards.	1
c.	(1)	2x Rim locks.[14]	2
	(2)	1x Rim & 1x mortice locks.[14]	2
	(3)	2x mortice locks.[14]	2
	(4)	2 x Padlocks.[14]	1
	(5)	Single lock.[14]	0
	(6)	Other lock(s).	-1

Sub total (a+b+c):

Section two score:

Notes:

(6) In accordance with JSP 440, Chapter 6, para 06210.

(7) The XPM should not be on external walls.

(8) In accordance with JSP 440, Chapter 6 para 06211(b).

(9) Lockable by means of a removable key.

(10) Frames with no rotten wood, brittle putty or other defect.

(11) Any defect effecting the overall integrity of the window.

(12) Such doors only score if the frame is in accordance with JSP 440, Chapter 6, para 06210(d)(3).

(13) In accordance with JSP 440, Chapter 6, para 06211(c).

(14) Of approved security pattern fitted at one-third and two-thirds down the locking edge of the door.

This page intentionally left blank

Section Three

SITE

1. **Situation of the building**. An index based upon additional security measures or weaknesses that affect the security of the building as a whole.

a.	Within an MOD site.[15]	25
b.	Within a government site.[2][15]	20
c.	Within a secure civil site.[2][16]	15
d.	Unguarded in a residential/industrial/commercial area where a crime watch policy exists.[17]	5
e.	Any other location.	0

Sub total:

2. **Compound Fences**. An index based upon a fenced perimeter with appropriate gates, all in good order.

a.	Within an anti-intruder fence/gates.	3
b.	Within a Defence Barrier standard fence (DWS SD50/1-5).	2
c.	Within a substantial barrier (non-security fence)	1

Sub total:

3. **Alarms**. A single score for an alarm, if fitted, to a building. To score the alarm must cover the storeroom/armoury where the weapons and ammunition are stored.

a.	Monitored alarm system	5
b.	Alarm with external sounder only.	2

Sub total:

Section three score:

Notes:

(15) Applies to any site with a full time security force.

(16) Applies to commercial/industrial sites with patrolled by a guard force and including such security measures as CCTV.

(17) To be checked and verified by the Security Unit during the survey.

2. **Total Index.** To calculate the total index add together the Section Scores. The final index is to include a positive score from Sections 1 and 2.

Total Index =

CHAPTER 7
COUNTER TERRORIST MEASURES

CHAPTER 7
SECTION I

COUNTER TERRORIST MEASURES

Introduction

07101. Threats to the security of MOD interests include espionage, terrorism, sabotage, subversion and organized crime. These threats change profile over time, reflecting the domestic and international scenes. The protective security system must therefore be capable of countering all elements of the threat.

07102. The term terrorism is applied to the activities of those organizations resorting to the use of violence and intimidation in the furtherance of political aims. Terrorist organizations have available the wide range of attack options detailed in Annex A. The threat to Service personnel and MOD civilian staff is under constant review. There may be a specific and higher threat to certain personnel because of past service or particular appointments.

07103. The MOD has a duty of care to ensure that proper arrangements exist for the protection of its personnel, weapons, equipment and property, wherever located. The purpose of this Chapter is to give general guidance for protection against terrorism. PSyAs and Command security staffs are responsible for providing detailed guidance on security procedures commensurate with the prevailing threat and the mandatory minimum standards of protection detailed in this chapter.

Terrorist Methodology

Terrorist Objectives

07104. Although their political aims may vary, terrorists have three common principal objectives:

a. To publicize their existence and cause.

b. To terrorize the community, thus coercing governments.

c. To discredit the authorities, possibly by provoking repressive counter measures.

Common forms of terrorist modus operandi are described at Annex A.

Non-Violent Extremists

07105. Non-violent extremist action directed at Defence interests often requires the commitment of resources to counter it. The measures outlined in this Chapter provide a sound basis for protection against such action. Anti-establishment demonstrations at non-nuclear MOD sites are generally of a minor nature and can be dealt with by local

resources. Non-violent extremist action at nuclear sites is sometimes on a larger scale but the guidance given throughout this Chapter remains applicable.

Threat Assessment and Dissemination

Threat Assessment

07106. Within GB, the threat to Service and MOD establishments from terrorism is assessed by the MOD Counter Extremist Advisory Group (CEAG). This assessment is based on intelligence provided by:

a. **Security Service.** The Security Service provides an assessment of the threat from Irish related terrorism and international terrorism.

b. **Metropolitan Police Special Branch (MPSB).** MPSB provide a resume, when appropriate, of Irish related terrorist activity in GB.

c. Defence Intelligence Staff (DIS). The DIS provide an assessment of Irish related terrorist activity in NI.

d. **Ministry of Defence Police (MDP).** The MDP, drawing on information from the National Public Order Intelligence Unit (NPOIU), provide an assessment of the threat from anti-nuclear and anti-arms groups and animal rights organizations.

07107. Using the intelligence received, the MOD CEAG provides a monthly terrorist threat assessment. This assessment is also used as the basis for setting the various BIKINI Alert States in GB. The assessment is based on a six-tier system of threat levels applicable to establishments, individuals and events. The definitions and terms for use in threat assessments have been agreed by ACPO for use by the civil police and national agencies. They aim to standardize terms used by all those concerned in assessing the terrorist threat and implementing counter-measures.

Level	Term	Definition
1	**IMMINENT**	Specific intelligence shows that a target is at a very high level of threat and that an attack is imminent.
2	**HIGH**	Specific intelligence, recent events or a target's particular circumstances indicate that it is likely to be a high priority and the target is at a high level of threat.
3	**SIGNIFICANT**	Recent general intelligence on terrorist activity, the overall security and political climate of the target's general circumstances indicate that it is likely to be a priority target and is at a significant level of threat.
4	**MODERATE**	A target's circumstances indicate that there is potential for it to be singled out for attack and it is at a moderate level of threat.
5	**LOW**	There is nothing to indicate that a target would be singled out for an attack and there is a low level of threat.
6	**NEGLIGIBLE**	A target is unlikely to be attacked. There is a negligible level of threat.

Northern Ireland

07108. Due to the volatile nature of the terrorist threat in NI, all assessment in this area of the UK is undertaken by personnel within the Province.

Overseas Theatres

07109. In overseas areas threat assessments are undertaken by in-theatre security committees and groups. These committees and groups are similar to the MOD CEAG and provide regional assessments of the current terrorist threat.

MOD Procedures for the Dissemination of Terrorist Threat Warnings and Information

07110. Within GB, there is a specific need to facilitate rapid response to intelligence and changes in Alert States. It is also essential that any information of activity that may be terrorist related be passed quickly and accurately to the appropriate agencies so that investigations are carried out. Rapid dissemination of warnings is achieved through the Focal Point System (FPS); other information is passed using the Suspected Terrorist Activity Reporting Procedure. Details of these systems and procedures are at Annex B.

The Focal Point System (FPS)

07111. The terrorist threat in GB demands a quick response to intelligence warnings or terrorist incidents. A key element of this response is the early dissemination of warnings and the exchange of information at all levels between the Services, MOD establishments and civil police forces, together with Foreign Service installations in GB.

07112. The FPS has been established in GB to meet the requirement for rapid dissemination of:

a. Urgent warnings of likely terrorist activity.

b. Information regarding real or possible terrorist incidents.

c. Urgent changes in the BIKINI or TESSERAL Alert States as ordered by the MOD, commanders or HOE on a local basis. The responsibility for co-ordination of the FPS is delegated by MOD to HQ LAND. It is fully described at Annex B.

Reporting and Collation of Suspicious Activity Considered Terrorist Related in GB

07113. The procedures to be used for reporting incidents that are considered to be suspicious and possibly related to terrorist activity but that by themselves do not meet the criteria for activating the FPS are also described at Annex B.

ANNEX A TO SECTION I TO CHAPTER 7

TERRORIST MODUS OPERANDI

1. When extremists use violence to further their political aims they are classified as terrorists. The tactics used by terrorist organizations vary with their objectives. The threat of violence to MOD personnel and property includes:

a. Rocket and bomb attacks, including petrol, nail, and acid bombs, intended to inflict casualties, cause major economic damage, disruption, discredit to security authorities or to gain publicity.

b. Booby traps, such as concealed improvised explosive devices (IED) (possibly incorporating delay timers ranging from a few hours to more than 30 days), or an under vehicle improvised explosive device (UVIED). Booby traps are used to harass and cause a diversion from other terrorist activity. They are also used in an attempt to murder, maim, intimidate, and lower morale generally.

c. Ambushes, ranging from small arms fire to co-ordinated multiple weapon attacks.

d. Sniping attacks at bases or at individuals outside establishments.

e. Mining of roads as an ambush or to cause disruption.

f. Use of direct and indirect fire mortars.

g. Raids to obtain weapons, ammunition, explosives or other stores.

h. Assassination, abduction and the holding of hostages.

i. Intimidation by all means ranging from threatening telephone calls to booby traps.

j. Hijacking of vehicles, aircraft or ships to seize hostages and to bring pressure on the government.

k. Attacks on aircraft on the ground and in the air to cause casualties and damage and to publicize terrorist offensive power.

l. Other incidents that cause embarrassment to HMG.

Terrorist Intelligence Activities

2. Terrorist organizations devote considerable effort to collecting intelligence. They use agents and informers and carry out covert observation and surveillance of establishments and individuals. They use technical equipment and are sometimes equipped with electronic devices for intercepting communications, particularly radio and telephone. Terrorists try to infiltrate government offices, customs posts, and even seek employment within establishments, where further opportunities for intelligence gathering may exist. They attempt to identify regular patterns of activity by establishments and individuals that disclose areas where the MOD is vulnerable, and where 'soft' targets exist. Detailed planning and preparation are likely to precede any attack.

Terrorist Weapons

3. Occasionally terrorists use large weapons such as improvised heavy mortars mounted and concealed inside vehicles, but they generally use weapons small enough to be concealed easily until the moment of use, or weapons that are capable of rapid assembly and breakdown. The armoury of well-organized terrorists normally includes collapsible weapons, light mortars, small rocket launchers, man portable air defence weapons and all types of small arms. They can be a mixture of professional manufacture or home made. Care is usually taken to husband weapons, particularly those that are regarded as prestigious, such as man portable air defence weapons and heavy calibre machine guns.

Use of Explosives

3. Terrorists use all types of manufactured and home-made explosives, sometimes in great quantities. They become skilled in concealing the movement of explosives by using specially adapted vehicles, suitcases, prams, carrier bags, and personal electronic equipment. They utilize a variety of equipment and techniques in the construction of improvised devices, examples of which are as shown below:

a. **Switches:**

(1) Simple release switches such as clothes pegs, activated by pulling a trip wire, operating the throttle lever of a vehicle, opening a door, or picking something up.

(1) Pressure switches triggered by stepping or sitting on something, or depressing an accelerator pedal.

(3) Cable switches set off by mechanical movement such as operating a manual choke of a vehicle.

(4) Time-delay mechanisms such as watches, clocks and clockwork and electronic timers, often used in IEDs and UVIEDs.

(5) Electronic switches, triggered remotely by a radio signal (remotely controlled improvised explosive devices (RCIEDs)).

(6) Tilt (mercury) and trembler switches set off by movement or inertia, and often used against vehicles, usually in conjunction with a time delay mechanism.

(7) Heat switches activated by, for example, a vehicle exhaust system.

(8) Light sensitive switches activated by, for example, exposure to light by removing a dustbin lid or discharging a photographic flash unit.

(9) Barometric pressure switches that operate on a change of altitude.

b. Improvised Explosive Devices (IED).

(1) Anti-personnel grenades thrown at security forces or placed as part of an ambush, sometimes containing nails or other improvised shrapnel.

(2) Devices concealed within or attached below a vehicle.

(3) Postal bombs ranging from a slim letter to a parcel.

(4) Incendiary bombs constructed, for example, inside a cassette box with a time-delay mechanism and typically placed in commercial premises and public transport.

(5) Cylindrical “pipe” bombs, using a wide range of different sized containers, for example, butane-gas cylinders, fire extinguishers and milk churns, packed with explosives.

(6) Stolen military ammunition modified for use as booby traps.

(7) Time delay IEDs using commercial or home made explosives packed into a car or truck.

This page intentionally left blank

ANNEX B TO SECTION 1 TO CHAPTER 7

THE FOCAL POINT SYSTEM AND SUSPECTED TERRORIST ACTIVITY REPORTING PROCEDURE

The Focal Point System (FPS)

1. The aim of the FPS is to ensure the rapid dissemination of information upwards, downwards and laterally, thereby facilitating quick reaction and mutual support between the Services, MOD establishments and the Armed Forces of other Nations in response to terrorist incidents or threats in GB.

Organization and Focal Point Plan

2. The FPS is based on groupings of Service and MOD establishments that lie within the geographical area of Army Divisional (including LONDIST)[1] and Regional Brigade boundaries. Responsibility for the overall co-ordination of the FPS, which is shown diagrammatically at Appendix 1, is delegated to HQ LAND. The arrangements for participation in the FPS by the Services and MOD establishments in peacetime are set out at Appendix 2.

3. The Army Divisional HQ is the Focal Point for that area and is responsible for co-ordinating and issuing a Focal Point Plan to cover all Service and MOD establishments located within the division's geographical boundary. Within a division's area, Service and MOD establishments are organized geographically into groups, and each group is co-ordinated by a specified Nodal Point. In areas where there are large concentrations of establishments it may be necessary to establish a third tier of co-ordination by using Sub-Nodal Points. Normally, Service HQ or major RN shore establishments, RM and Army units or RAF stations are nominated as Nodal and Sub-Nodal Points.

4. Divisional Focal Point Plans ensure that a simple unclassified message can be relayed within one hour (in most cases by telephone) from any location within a division's area to a point of contact for every other establishment throughout a division's geographical area.

[1] LONDIST is the only District within LAND. For the remainder of this Annex when Divisions are mentioned LONDIST is included.

Reporting Incidents

5. In the event of a terrorist incident or suspected incident, which necessitates urgent notification to local establishments, e.g. within the node, or when a local assessment is made which causes an establishment to raise the BIKINI or TESSERAL Alert State or to increase the counter measures in force, reports are to be made as follows:

a. **To the civil police.** The civil police have prime responsibility within GB for dealing with terrorist incidents, including hoaxes, on MOD property and it is **essential** that the local civil police are informed immediately.

b. **MOD Reporting Chain**

(1) **TLBs.** Reports are to be made to the appropriate PSyA and Command security staffs. PSyAs are to ensure that all reports of terrorist related incidents and changes to Alert States are passed immediately (usually by telephone) to D Def Sy. Confirmatory signals are to be sent to the appropriate HQ and MODUK (D Def Sy) using SIC 'YPL'.

c. **Through the FPS.** In the event of a terrorist incident, actual or suspected, or when an Alert State has been changed based on local assessment:

(1) The establishment, unit or station concerned is to notify its associated Sub-Nodal or Nodal Point and all other establishments to whom it has a responsibility to pass information under the FPS.

(2) The Sub-Nodal Point, where there is one, is to inform its associated Nodal Point and all other establishments to whom it has a responsibility to pass information under the FPS.

(3) The Nodal Point is to inform its associated Focal Point and all other Sub-Nodal Points and establishments to which it is required to pass information under the FPS.

(4) The Focal Point is to inform HQ LAND and if it is considered necessary other Nodal Points to which it has a responsibility under the FPS as considered appropriate.

(5) HQ LAND is to inform MOD and the following: CINCFLEET, 2SL/CINCNAVHOME, HQ STC, PJHQ, HQ DLO and, if it is considered necessary, other Focal Points in GB as appropriate.

Awareness of the System

6. The effectiveness of the FPS will depend largely on duty personnel manning telephones, on a 24 hour basis, being aware of the system and being able to implement it. To this end:

a. All HQ, establishments, units and stations are to nominate day and night contact telephone numbers that are permanently manned. Where this is considered

to be impossible, dispensations are to be sought from the appropriate PSyA and Command security staff.

b. All personnel liable to man duty telephones in establishments within the FPS are to be briefed on the system as it affects them and on their responsibilities for making it function. In most cases, this will involve clearly displayed simple instructions on the action to be taken in the event of a terrorist incident and a list of telephone numbers to which the initial reports are to be passed.

c. All personnel are to be aware of the need to pass information accurately, clearly and concisely.

Coordination

7. **Chain of command.** The FPS complements established single-Service and MOD chains of command, which should normally be used for the passage of single-Service reports to and from MOD.

8. **Mutual support.** In the event of a terrorist incident, the co-ordination of emergency assistance is the responsibility of the civil police. In cases of urgent need, mutual support may be requested and provided on a local inter-Service basis using the Focal Point communications channels.

9. **Alert state changes.** It remains the prerogative of single-Service commanders to decide whether to raise Alert States or to increase counter measures in particular areas within GB in response to a locally perceived threat. Such changes are to be reported to D Def Sy.

10. **Practices.** HQ LAND will co-ordinate the practices of the FPS to involve all units and establishments not less than twice annually in consultation with the appropriate PSyAs where MOD HQ, DPA and DSTL establishments are involved and CINCFLEET, 2SL/CINCNAVHOME HQ STC, PJHQ and DLO for their respective establishments, units and stations. They will also inform D Def Sy. These exercises are known as **Exercise Rapid Call.**

11. **Amendments.** Any changes to the FPS that appear to be necessary as a result of its use are to be reported through PSyA channels to HQ LAND who will inform D Def Sy.

12. **Application in TTW and War.** In TTW and war, the FPS will be expanded to include the exchange of intelligence on all matters relevant to the defence and continued function of all establishments involved in the system. It will be activated by MOD. Army Division and Regional Brigade HQ will continue to act as Focal Points, but TAOR HQ, when activated, will take over the responsibilities of Nodal Points for all establishments within the TAOR. Details of the Wartime Focal Point System are in Part 1 of the United Kingdom Commanders-in-Chief Committee MHD Plan.

Reporting of Suspicious Incidents

13. **Aim.** The aim is to establish Joint Service, MOD (including MOD HQ, DPA, DLO, DSTL and MDP procedures for the passage and collation of reports of suspected terrorist related activities.

Definitions

14. To ensure common understanding of some definitions and application of these instructions, a number of terms need to be defined. These are:

a. **Suspected terrorist related activities.** Suspected terrorist related activities are activities that fall short of the criteria for initiating the FPS; examples are:

(1) A vehicle, or persons, acting suspiciously in or near Service Families Accommodation.

(2) A conversation overheard, or an action seen in a public place, that clearly pointed to possible wrong doing or was of a highly suspicious nature.

(3) Receipt of a bomb threat warning.

(4) Service dependant's visitor who has been acting strangely or asking suspicious questions.

(5) Suspicion regarding the occupants of a house or flat close to an MOD installation.

b. **Unit level, intermediate level, command level.** Due to the differing Service Command chains, the following terms are used:

(1) **Unit Level.** This will include MOD, Service, DPA, DLO and DSTL establishments.

(2) **Intermediate Level.** This applies to Naval Base or Naval Air Station Commanders, HQRM (if RM units are involved), Army Divisional HQs (through Regional Brigade or area HQs as appropriate), RAF P&SS Regions and MDP Divisional HQ.

(3) **TLB Level.** CINCFLEET, 2SL/CNH, CINCLAND, AG, CINCSTC, PTC, PJHQ, CDL, CDP, and MOD Centre.

c. **Focus.** This is the focus of the collation activity that supports a particular Service or TLB. They are as follows:

(1) **RN and RM.** DNSyICP.

(2) **Army.** 2 MI Bn.

(3) **RAF.** HQ P&SS.

(4) **MOD Centre.** CB (Sy)1.

(5) **MDP.** MDP Force Information Room.

(6) **CCRIO RMP.** Whilst not a Service security focus, CCRIO RMP is heavily involved in the investigation of suspect or stolen vehicles.

d. **Resolved.** This term implies that investigations show that the reported activities are not terrorist-related or have been pursued to a reported conclusion.

Reporting Procedures

15. **Individuals.** All personnel, both Service and civilian, and their dependants are to be instructed to report any activity that arouses their suspicions, however trivial it may seem, without delay. Reports are to be made as follows:

a. To the designated reporting point (e.g. main guardroom, MDP security control room, or ESyO) if the activity occurs within a MOD establishment or very close to it.

b. All other suspect activities are to be reported immediately to the civil police using 999, followed by a report to a Service reporting point, e.g. an individual's unit, nearest Service unit or the MDP.

16. **Unit Level.** On receipt of a report, the unit is to:

a. Ensure that the civil police are immediately made aware of the reported suspect activity, particularly that to which an operational response by them appears necessary.

b. Telephone an immediate report of the suspicious activity to the appropriate intermediate level. Telephoned reports must be corroborated by signal or fax, with information copies to the relevant HQ, as well as CCRIO RMP if suspect or stolen vehicle are involved.

Follow up of Reports of Suspected Terrorist-Related Activity

17. **Intermediate Level**. The appropriate security units in conjunction with the civil police and the unit are immediately to investigate the circumstances leading to the report. This is to confirm the original facts reported with a view to:

a. Determining whether any additional protective measures are needed, such as an increased Alert State or activation of the FPS.

b. Helping to assess similar reported activities or trends.

c. Closing the case as resolved or deciding that no further progress can be made at Intermediate Level. Progress in the investigation is to be reported to the relevant TLB, as well as to CCRIO RMP if suspect or stolen vehicles are involved. Unless there are good reasons to the contrary, the security focus that initiated a report is to lead on any follow up activity. Any incident that gives cause for concern, or appears to correlate with information from another TLB is immediately to be passed to the other relevant security focus, MDP Force Information Room and CCRIO if suspect or stolen vehicles are involved. Close liaison is to be maintained with the civil police, and the other security focus that may be approached for help direct. The relevant PSyA and Command security staffs are to be advised of the progress of the investigation. Investigations are to continue until the case is **resolved** or it is decided that further investigation is fruitless.

18. **TLB Level.** If a wider dissemination is deemed necessary, the reports (or gist of them) with comment from security staff, if appropriate, are to be passed to all the other TLBs and security focus. CCRIO RMP should be included if suspect or stolen vehicles feature in the report. Reports of significant incidents are also to be passed to MOD D Def Sy.

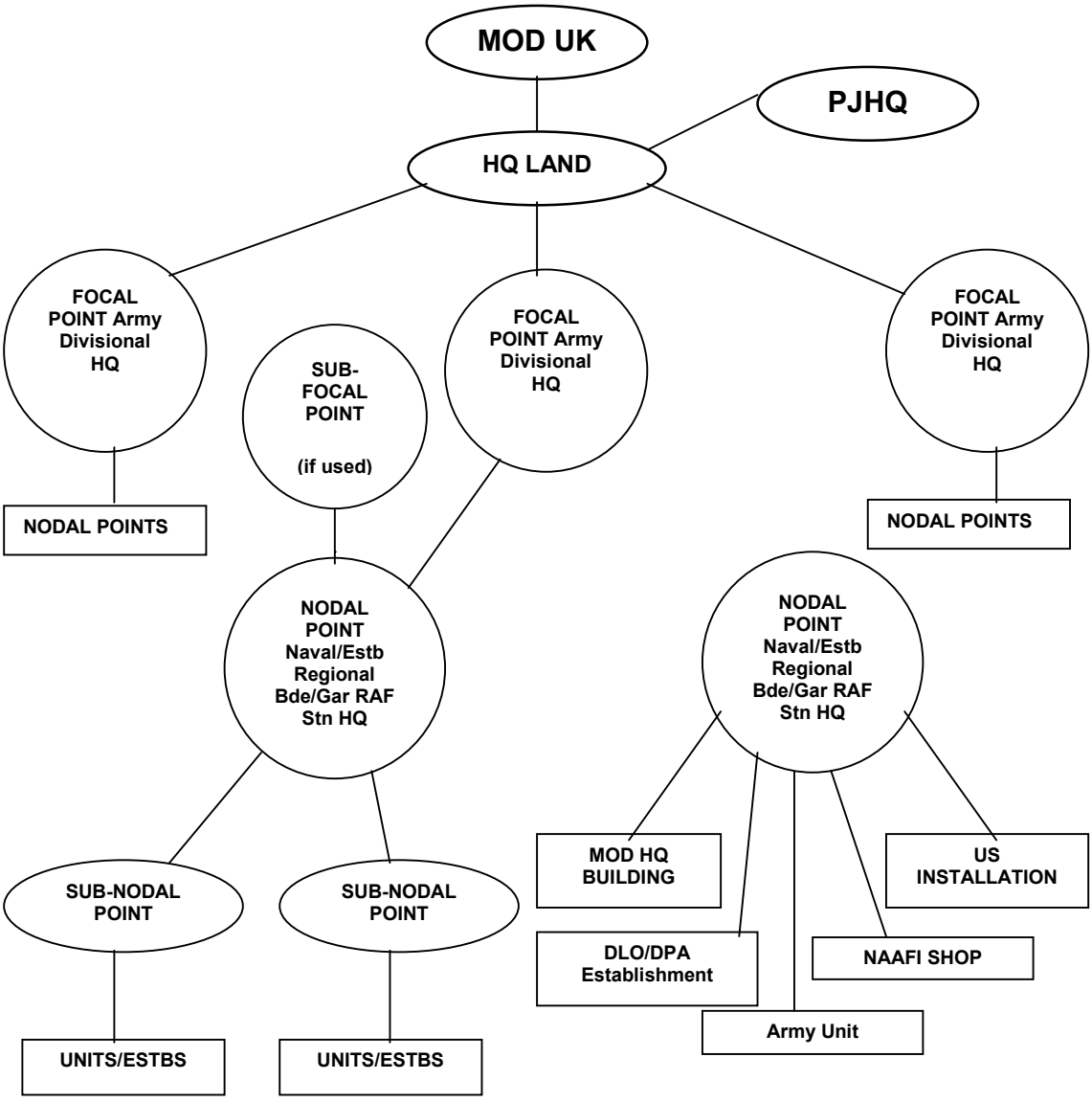
19. **MOD Action.** D Def Sy will monitor ongoing cases and where appropriate prepare briefs for Central and Ministerial staffs. D Def Sy will disseminate relevant details to national agencies. A monthly summary of reporting activity will be produced for discussion at the MOD CEAG.

20. **CCRIO RMP Action.** In addition to its current task, CCRIO RMP will review the reports it receives of suspect or stolen vehicles with a view to discovering similarities in reports stemming from independent sources. This is opposed to follow-up reports on vehicles about which it had already disseminated information. Any such similarities are to be drawn to the attention of the security focuses from which the independent reports originated. This will allow further investigation if considered necessary.

APPENDIX 1 TO ANNEX B TO SECTION I TO CHAPTER 7

FOCAL POINT SYSTEM

1. The Focal Point System (FPS) is designed to facilitate the rapid dissemination of information up, down and laterally along the chain of command. A schematic example is given below:



This page intentionally left blank

APPENDIX 2 TO ANNEX B TO SECTION I TO CHAPTER 7

PARTICIPATION IN THE FOCAL POINT SYSTEM

1. **The Royal Navy.** DNSyICP is the point of contact concerning Focal Point arrangements. Subordinate RN/RM HQ, shore establishments and units may be used as Nodal Points.

2. **The Army.** The responsibility for co-ordinating arrangements for the Focal Point System is delegated to HQ LAND. Army Divisional HQ are used as Focal Points and are to co-ordinate the Focal Point arrangements within their geographical boundaries.

3. **The Royal Air Force.** RAF stations and units may be approached direct through SSyOs on matters concerning Focal Point arrangements, keeping the relevant RAF Command HQ informed. RAF stations may be used as Nodal Points.

4. **US Forces based on RAF stations.** Liaison with US Forces based on RAF stations is through the RAF commander.

5. **Other Allied Forces.** Liaison with allied forces (other than US Forces based on RAF stations) is through the controlling formation HQ of the Service with whom the allied forces are stationed. In the event of an allied base being the responsibility of a department other than one of the Services then advice is to be sought from MOD as to the correct method of liaison.

6. **MOD HQ Buildings.** Liaison is direct to the appropriate Building Controller.

7. **DLO.** Where a DLO unit is a lodger unit, liaison is to take place through the host establishment, otherwise liaison is to take place directly with the Director/Head or Security Officer of the DLO establishment concerned.

8. **DPA.** Where a DPA unit is a lodger unit on a Service establishment, liaison is to take place through the host establishment, otherwise liaison is to take place directly with the Director/Head or Security Officer of the DPA establishment concerned.

9. **MDP.** MDP detachments conform to the arrangements agreed by their parent establishments.

9. **NAAFI.** Army Divisional and Regional Brigade HQ are to liaise direct with NAAFI regional managers for the inclusion in the Focal Point System of NAAFI premises outside Service establishments.

This page intentionally left blank

SECTION II TO CHAPTER 7

PRINCIPLES OF COUNTER TERRORIST PROTECTION AND THE MOD COUNTER TERRORIST STRATEGY

Principles of Protection

07201. The principles of protection against terrorist attack are:

a. Timely dissemination of the assessed threat and maintenance of an appropriate Alert State by units and personnel.

b. Initiation of appropriate response mechanisms to deal with rapid changes in the Alert State.

c. Deterrent measures, such as:

(1) Defence in depth.

(2) Armed posture.

(3) Constant review and improvement of physical security.

(4) Effective personal security.

(5) Security education programme for all MOD personnel.

The MOD Counter Terrorist Strategy

07202. To ensure that the above principles are applied throughout the MOD and that clear, long term, goals are set and promulgated in order that appropriate LTC funding can be allocated for physical security measures, security training and awareness programmes.

Action to Counter Terrorist Attack

Individual Vigilance

07203. The key factor in countering the threat of terrorist violence is a high state of vigilance by all personnel. Every individual needs to be aware that the threat of terrorist attack is real and that protection is best achieved by being alert, suspicious and vigilant, at all times, both on and off duty. Such alertness is comparatively easy to maintain following a well publicized act of terrorist violence, but is difficult to sustain during quieter periods. Every opportunity must therefore be taken to remind everyone of the need to be vigilant, and to be seen to be vigilant. Efforts should be made to raise the level of awareness of the general public living adjacent to MOD establishments and involve them in the need for vigilance.

07204. Action to counter terrorist attack is based on:

a. Assessing the threat (see paragraph 07106).

b. Maintaining the Alert State (see paragraphs 07301 to 07309).

c. Establishing sound systems of protection in Service establishments (see Section IV).

d. Protecting High Threat Personnel (HTP) (see Section V paragraphs 07509 to 07515).

MOD Counter Terrorist Organization

Introduction

07205. Service establishments and personnel have traditionally been viewed as attractive and legitimate targets by Irish republican and other terrorist organizations. In order to counter these and other threats that may arise, the MOD has developed a responsive counter terrorist organization. The organization extends from Whitehall to establishments, through PSyAs and Command security staff, and is assisted by security units and the civil police. Co-operation throughout the MOD has resulted in a joint approach to counter terrorism, which is outlined below.

MOD Directorate of Security Policy (D Def Sy)

07206. D Def Sy and is responsible for setting and monitoring security policy for the MOD. D Def Sy promulgates the Alert States for the MOD in Great Britain and is responsible for the dissemination of threat information world-wide.

MOD Counter Extremist Advisory Group

07207. Within MOD, the CEAG is the focus for all counter terrorist and extremist matters in UK, excluding NI.

07208. The main purpose of CEAG is to receive and consider assessed intelligence on current or future terrorist and extremist activity from both indigenous and international threats which are of concern to defence interests world-wide. CEAG usually meets on the first Wednesday of each month and issues an extremist threat assessment signal. Should any new intelligence become available or terrorist incidents occur between the regular meetings, the CEAG would meet in special session. All members of the CEAG are on call at all times. The CEAG also provides, when necessary, members for 'ad hoc' working groups to consider and approve joint counter terrorist policy.

Passage of Warnings

07209. In Great Britain, at Ministry of Defence level, warning of possible terrorist activity may be received from the Security Service, the Metropolitan Police Special Branch or other sources at any time. These reports are handled as follows:

a. **During Working hours.** Warnings are passed to the CEAG Secretary. The CEAG considers the assessment received and, through D Def Sy, passes the assessment and any change in the Alert State to the MOD.

b. **During non-working hours.** Warnings are passed to the Defence Crisis Management Centre (DCMC). DCMC informs the CEAG Secretary who arranges for a reassessment to be made by members of the CEAG if required. The DCMC disseminates any change in the Alert State to the MOD on authority of the chairman of the CEAG. In the event of immediate danger to life, the DCMC Duty Officer may issue instructions on his own authority, informing DCDS(C) and the CEAG Secretary as soon as possible.

07210. Commands and HQNI are responsible for laying down their own procedures for passing warnings to formations.

Liaison with the Security Service and the Metropolitan Police Special Branch.

07211.

a. D Def Sy is responsible for liaison with the Security Service and the Metropolitan Police Special Branch on behalf of the MOD.

b. Liaison overseas is dealt with at sub-paragraph 07109.

TLB Holders Responsibilities.

07212.

a. **Division of staff responsibility.** The responsibility for ordering protective measures against terrorist attack is vested in the operations staff. PSyAs and Command security staff are responsible for providing assessments of the threat from terrorism, and for the planning and co-ordination of protective security measures to counter the threat.

b. **Assessment of the threat.** For Great Britain and overseas threat assessments are disseminated by the CEAG Secretary. In NI assessments are made and disseminated by HQNI.

c. **Guidance on security measures.** TLBs are responsible for issuing guidance and instructions to subordinate establishments on the counter terrorist measures to be taken.

Establishments

07213.

a. **The local threat.** HOE are responsible for assessing the vulnerability of their own establishment and for keeping the threat to their personnel, weapons,

equipment and property under review. They are given the authority to declare a higher Alert State and additional measures in response to a local emergency – PSyAs and Command security staff are to be informed of such action.

b. **Implementation of security measures.** HOE must take all necessary measures to ensure the safety and security of their personnel and installations, based on the instructions issued by superior HQ, taking into account their own assessment of local circumstances.

c. **Briefing and training.** HOE must ensure that all Service personnel and MOD civilian staff are briefed regularly on the threat, the security measures that they need to know and, most importantly, the need for vigilance at all times. Security routines, particularly those concerned with the safety of personnel, must be practised.

d. **Liaison with the civil police.** In Great Britain establishments are to maintain liaison with their local police except where this is done under collective arrangements, e.g. by a neighbouring garrison or HQ. HOE overseas are responsible for issuing appropriate instructions.

e. **Reporting of incidents.** HOE must report immediately all incidents concerning the terrorist threat, however minor, to their superior HQ and as appropriate, through the Focal Point Scheme.

Plans and Training

07214. HOE are responsible for the production and maintenance of an up-to-date, comprehensive security plan, which is to include a joint contingency plan with the police and emergency services for handling terrorist incidents. They are also responsible for ensuring the regular briefing of all Service personnel, civilian employees and dependants on the terrorist threat. In addition, they are to ensure that all Service personnel and civilian employees receive sufficient protective security training to allow them to carry out their establishment security duties effectively and protect themselves from terrorist attack while on and off duty. HOE should seek specific advice from their establishment security staffs, security units, MDP and MGS (if appropriate), and from their PSyA or Command security staff.

Inter Service Security Committee (ISSC)

07215. The ISSC is a Command level forum for the discussion of all security matters that may affect the Services in GB. It acts as focus for the exchange of ideas and as a co-ordinating body for the implementation of security policy, security education and the staffing of proposals to MOD, such as matters raised at the higher level CEAG.

Search Working Group (SWG)

07216. Counter terrorist search (CTS) involves the use of systematic procedures to find terrorists and their resources and to confirm the presence or absence of bombs within specified boundaries. Objectives of CTS include obtaining evidence, depriving terrorists

of their resources, providing information or assuring a facility is safe to use. The MOD SWG assists the Joint Service Search Policy and Resources Committee (JSSPRC) to develop search techniques and procedures and identify requirements for manpower and equipment. The SWG is currently in abeyance and will be resurrected if required. In the meantime, the work of CTS is carried forward by the JSSPRC.

Funding

07217. Funding for all physical security measures is provided by the appropriate TLB holder. The guidance in this document must therefore be applied by PSyAs and Command security staffs, balanced against their other commitments. If in the event of a significant change in the terrorist threat additional security enhancement funds become available on a centrally funded basis they will be allocated on a priority basis.

Responsibilities of the Security Service and the Civil Police for Counter Terrorist matters in GB

Civil Authorities

07218. The primary responsibility for the maintenance of the Queen's Peace, the prevention and detection of crime, the protection of life and property and the prosecution of offenders (in support of the prosecuting authorities) rests with the civil police; any such incident or suspicious activity must, therefore, be reported to the civil police immediately. In practice, because of the heavy burden on civil police resources, the Services are required to accept responsibility for the protection of their own personnel and dependants within establishment perimeters. Establishments must maintain liaison with the local police on such matters as:

a. The local threat.

b. Security plans involving action both on and off Ministry of Defence property.

c. Establishment security measures that may affect the public.

d. The security of military personnel in local places of entertainment and when using public transport.

e. Post incident control.

The Security Service

07219. The Security Service is the lead Government Service for the collation and assessment of information relating to all terrorist threats in GB. The Security Service works closely with the Metropolitan Police Special Branch (MPSB) and with the Special Branches of other forces as required.

The Home Office for England and Wales and the Home and Health Department for Scotland

07220. The Home Office for England and Wales and the Home and Health Department for Scotland are responsible for the promulgation of policy on terrorist matters relating to the civil police.

Civil Police

07221. In the civil police each constabulary or force is commanded by a Chief Constable who has autonomous responsibility for all civil police counter terrorist operations conducted within his jurisdiction. The Association of Chief Police Officers (ACPO) and its Scottish Counterpart ACPO(Scotland) provide a national forum for the discussion of Home Office policy and represent the 51 police forces in GB. The ACPO committee on terrorism and allied matters specifically discusses anti-terrorist matters. Within individual forces, the Assistant Chief Constable Operations (ACC Ops) is usually responsible for operational control of counter terrorist operations.

Investigation of Terrorism

07222. The investigation of terrorism is carried out by the appropriate civil police CID. In the case of Irish republican terrorism, the Metropolitan Police Anti-Terrorist Branch (SO13) has a co-ordinating role.

Joint Service Police Committee (JSPC)

07223. JSPCs are established at Force, Divisional and Sub-Divisional level. Their function is the co-ordination of common security matters and procedures, the exchange of relevant security information and the review of joint police and Service security plans. Representation is as follows:

a. **Force**.

(1) Police - Chief Officer.

(2) RN/RM - As considered appropriate.

(3) Army – GOC or Brigade Commander.

(4) RAF - A senior provost officer appointed by OC HQ RAF P&SS.

a. **Divisional**.

(1) Police - Divisional Commander.

(2) RN/RM - Establishment commander.

(3) Army – Garrison or establishment commander.

(4) RAF - Station Commander(s) or officer from the appropriate RAF P&SS Region.

b. **Sub-Divisional**.

(1) Police - Sub-Divisional Commander.

(2) RN/RM - Establishment commander.

(3) Army - Garrison or establishment commander.

(4) RAF - Station Security Officer.

This page intentionally left blank

SECTION III TO CHAPTER 7

TERRORIST ALERT STATES

General

07301. The MOD terrorist Alert States are the foundation of counter terrorist security precautions for all MOD personnel, the Alert States also provide maximum commonality with other Government Departments. Overseas commands have similar Alert States although they may be known by different codewords. They all provide controlled, measured and standardized responses to the various terrorist threats applicable to the MOD. The systems are concerned with:

a. Warning of possible terrorist activity.

b. Measures to be taken upon receipt of a warning.

07302. Establishments are to be prepared to change from one Alert State to another at short notice.

Alert States

07303. The following codewords are used to convey warnings of possible terrorist activity:

a. **BIKINI.** Used to warn of non-specific forms of terrorist activity.

b. **TESSERAL.** Used to warn of a threat of terrorist use of surface to air missiles (SAM) or anti-aircraft machine guns (AAMG) against Service aircraft.

c. **KEENWIND.** Used to warn of non specific forms of terrorist activity in BFG (see paragraph 07309).

Definitions and Alert Measures

07304. The definitions and countermeasures associated with the individual Alert States are detailed as follows:

a. MOD BIKINI Alert State system - Annex A.

b. MOD TESSERAL Alert State system - Annex B.

07305. BIKINI Alert State System

a. The Alert State is decided by the Cabinet Office and is normally applicable across all Government Departments. In the MOD, the CEAG considers the BIKINI Alert States and related countermeasures and, through D Def Sy, represents the MOD view to the Cabinet Office. Exceptionally, MOD may apply a higher Alert State if the threat is directed at Defence interests. The assessed threat of terrorist attack will continue to be promulgated routinely by CEAG to both GB and overseas commands and theatres. In the UK the Alert State will be issued by the CEAG, following discussion with other Government Departments. In overseas commands,

the in-theatre Joint Security Group (JSG) takes into account the threat level issued by CEAG, as well as regional and in theatre assessments of the current terrorist threat, and decides the Alert State.

b. There are five Alert States: WHITE, BLACK, BLACK SPECIAL, AMBER and RED in ascending order of threat level. BIKINI WHITE is the first and lowest of the five BIKINI Alert States and provides the foundation of countermeasures for all higher Alert States, including those of the declared Alert State as invoked in the relevant command or theatre; e.g. BIKINI BLACK SPECIAL would also incorporate the countermeasures of BIKINI BLACK. Where countermeasures refer to similar actions, those imposing the highest standard take precedence. The definitions of the BIKINI Alert States are at Annex A. The BFG KEENWIND Alert State System used in Germany, Belgium, France and the Netherlands mirrors the BIKINI Alert State colours and definitions.

c. The countermeasures for each BIKINI Alert State are given at Appendices 1-5 to Annex A. CEAG and JSGs may also determine that additional countermeasures from within the BIKINI system are appropriate to the threat and add these to the mandated BIKINI countermeasures at each level of the Alert State, promulgating them on a monthly basis. Additional countermeasures over and above those within the BIKINI system can also be developed by overseas commands, depending on local circumstances, and promulgated on a local basis, bearing in mind the need to achieve a security posture broadly compatible with the relevant BIKINI Alert State. Note that the BFG KEENWIND countermeasures, which are not necessarily tied to Alert States, differ substantially from the BIKINI system.

d. Unless the threat assessment indicates otherwise, all establishments should adopt the same Alert State and countermeasures. Additional countermeasures in individual TLBs and Commands may also be applied where appropriate and registered with CEAG. The Alert State and associated countermeasures ordered by CEAG or JSGs are to be regarded as minimum mandatory standards. Where, for practical reasons, an establishment is unable to implement a particular counter measure the Head of Establishment is to consult the appropriate PSyA through the chain of command and alternative compensating countermeasures are to be applied where practicable.

Promulgation of the Threat and Alert State

07306. Terrorist threat assessments, BIKINI Alert States and applicable countermeasures will normally be promulgated by CEAG through D Def Sy, Service chains of command and, where appropriate, through the Focal Point System. Exceptionally, in the face of imminent increased terrorist threat, an establishment or formation has reason to believe that at any time it is subject to a higher threat than elsewhere, then it may raise the Alert State locally or enhance the countermeasures locally. Such action should be reported as soon as possible to the MOD through the normal chain of command keeping all other interested establishment and formations informed as appropriate.

Counter Terrorist Physical Security Measures for MOD Buildings

07307. Counter terrorist physical security measures are to be applied to all MOD owned or occupied buildings, the purpose of which is to limit damage to the building fabric and injury to the occupants. It is the responsibility of PSyAs and Command security staffs to ensure that the measures applied are appropriate and take into account the location and function of the building. The minimum physical security measures are given in Chapter 5 Section II Annex G.

Protective Marking of Alert States and Measures

07308. The protective marking of the definitions of the BIKINI Alert States is RESTRICTED but the codewords BIKINI WHITE, BIKINI BLACK, BIKINI BLACK SPECIAL, BIKINI AMBER and BIKINI RED are not protectively marked. These codewords may be passed by telephone provided that they are not qualified in any way. Notices displaying the current Alert States are to be sited so as to minimize the likelihood of the general public seeing them. These codewords and their meanings are understood by the civil police. The codewords and their definitions are not to be communicated to the media or any other unauthorized person.

Overseas Alert States

07309. With effect from 1 Jan 01 the codeword BIKINI, with the associated colour coded Alert State definitions and suites of countermeasures, is used throughout MOD and in all overseas commands and theatres with the exception of British Forces Germany (BFG). In Germany, Belgium, France and the Netherlands the BFG KEENWIND codeword and its associated mandatory, random and discretionary countermeasures will be retained but using the BIKINI Alert State definitions and colour codes. From 1 Jan 01 the codewords RIPPLE (Cyprus), ROCK (Gibraltar), TONGA (Turkey), NOMAD (Bahrain, Kuwait and Saudi Arabia) and GLACIER (Falkland Islands) are no longer to be used and are replaced by BIKINI. In overseas commands, the appropriate in-theatre security committee or Joint Security Group (JSG) takes into account the threat level issued by CEAG, as well as regional and in theatre assessments of the current terrorist threat, and decides the Alert State. Before deployment, units are to be informed by the appropriate PSyA through the chain of command of the current BIKINI or BFG KEENWIND Alert State and the associated countermeasures required in theatre.

Overseas Terrorist Threat Assessment List

07310. D Def Sy in conjunction with DI(TILS) and the Security Service provide a threat assessment for those overseas areas to which the Services deploy on a regular basis. This assessment is known as the Overseas Terrorist Threat Assessment List (OTTAL) and includes US threat levels world-wide.

07311. The OTTAL is updated on receipt of new intelligence that affects changes in threat levels. Amendments are issued by signal to Defence Attaches and TLBs. Personnel deploying overseas are to ensure that they are aware of the threat in the country to which they are travelling.

Division of Responsibilities for Protection Overseas

07312. The nature and extent of MOD responsibility vis-à-vis that of the civil police in overseas commands and establishments varies considerably. In some cases working arrangements with the civil police may be similar to those in the United Kingdom. Where there is inadequate civil police support, the MOD may be entirely responsible for the security of UK personnel. However, in commands such as UKSC(G) the civil police may have complete jurisdiction outside the actual confines of establishments. The local operations staff is responsible for ensuring that the division of responsibilities is clear.

The Carriage of Weapons and Employment of Armed Personnel on Security and Police Duties in Peacetime

Authority and Responsibilities for Arming

07313. Routine arming of guards is authorized by the MOD, with Ministerial approval, although there are prescribed circumstances which automatically require arming (see below). CINCs are responsible for operational armed guard deployments at establishments under their command, and will personally issue written arming authorities and authorize ROE as appropriate in accordance with MOD direction, promulgated in Joint Service Publication (JSP) 398 2000 Edition - UK Compendium of National Rules of Engagement.

Circumstances for Arming

07314. CINCs may authorize the carriage of arms and ammunition by suitably trained and qualified Service personnel for general security duties when the BIKINI Alert State is BLACK, BLACK SPECIAL, AMBER or RED.

07315. The HOE at any installation may authorize the arming of Service personnel if there is a substantive or immediate threat to the establishment. Ministerial approval is to be sought retrospectively through the chain of command without delay. The arming of personnel on nuclear weapons security duties is to be in accordance with JSP 440 Volume 4.

Civil Police Jurisdiction

07316. The primary responsibility for maintaining law and order and the internal security of the UK rests at all times with the civil authority, normally represented by the civil police. The Armed Forces, which are subject at all times to the direction and control of HM Government must, when operating in the UK, comply with the law and act in support of the civil authority. Civil police primacy is therefore to be respected and the Armed Forces will only take responsibility when the civil police assess that they do not have the capability or resources to deal with particular situations. Even then, responsibility will be transferred to the military for the minimum period of time necessary to enable effective action to be taken to preserve life. The Chief Constable must therefore give his formal agreement to any proposal to deploy Service personnel or MDP outside Service establishments.

Weapon States

07317. Weapons are **not** to be issued without ammunition. There are 3 possible arming states for general use:

a. **State 1 - Unarmed.** At State 1, firearms and live ammunition are to be held in the guardroom or other specified location in such a way as to be available in the event of an emergency.

b. **State 2 - Armed (Prepared).** At State 2, firearms are to be carried with loaded magazines held in the ammunition pouch.

c. **State 3 - Armed (Alert).** At State 3, firearms are to be carried with a loaded magazine on the weapon, and the weapon made safe.

Reporting of Incidents

07318. Commanders are to report any serious incident involving armed personnel, through the normal chain of command without delay. Any rounds discharged inadvertently in the preparation for, conduct of or dismissal from, armed security duties are to be treated as negligent discharges and are to be reported accordingly.

Warning Notices

07319. Notices warning of the presence of armed guards are not to be posted.

Questions on the Arming Posture - Public Relations (Media Liaison)

07320. Questions from the public or media about the arming posture at particular establishments are normally to be referred to command Media Ops staff. Unless there are special factors that require the MOD to be consulted, questions should normally receive the reply: "It is not MOD practice to comment on security arrangements. These arrangements are kept under review".

Employment of Armed Personnel on Security Duties

07321. HOE are responsible for the security of their establishment and personnel. In practice, the ESyO will be responsible through the normal chain of command for the implementation of all routine security measures and practices to combat terrorism.

Rules of Engagement

07322. The ROE for the use of firearms in peacetime within GB are to conform to the Joint Service Publication (JSP) 398 2000 Edition - UK Compendium of National Rules of Engagement. HOE are to promulgate ROE in standing orders. All personnel are to receive adequate training.

Combat Body Armour and Combat Helmets

07323. At BIKINI BLACK SPECIAL (or BLACK 'ARMED') it is not mandatory for armed counter terrorist security personnel to wear specialized equipment such as combat body armour or combat helmets. However, at BIKINI AMBER or RED all personnel employed on armed counter terrorist security duties outside protected buildings should wear combat body armour together with a combat helmet where these are available.

Batons

07324. Detailed policy on the issue and use of batons by Service Personnel is at Annex D to this Section. Authority for the issue of batons is as follows:

a. **Operations**. Requests to issue and use batons on operations are to be made through the ROE process.

b. **Security.** Standing authority is granted to CINCs for the issue and use of batons to personnel deployed on security duties. CEAG is to be informed when batons are issued for security purposes.

Training

07325. Batons should only be issued to appropriately trained personnel. The single Services are responsible for determining the scale of the training requirement and for the implementation of suitable training. Minimum training standards are mandated at Appendix 1 to Annex D. Auditable records of training are to be kept.

Guidance on the Use of Batons

07326. Short of armed conflict, batons are to be used in accordance with English law. ROE for the use of batons is at Appendix 2 to Annex D

ANNEX A TO SECTION III TO CHAPTER 7

MOD BIKINI ALERT STATES - DEFINITIONS

1. **General.** There are five BIKINI Alert States[1] which, in ascending order of severity, are listed and defined below.

2. **BIKINI WHITE.** No specific threat. This Alert State provides for a minimum level of security appropriate to the ever-present global risk of terrorism and violent extremism.

3. **BIKINI BLACK.** It is assessed that there is a **possibility** of terrorist activity with no defined target or time of attack. The minimum Alert State to be applied while Irish republican and other terrorist organizations are assessed as a potential threat in Great Britain or overseas and have the capacity to revert to operations during the period of a cease-fire.

4. **BIKINI BLACK SPECIAL.** Information has been received and it is assessed that there is an **increased likelihood** of terrorist activity with no defined target or time of attack. This Alert State would normally be applied when the assessment indicates an increased threat that does not justify adopting BIKINI AMBER. It may also be applied as a precautionary measure for short periods to cover events liable to stimulate terrorist action.

5. **BIKINI AMBER.** Specific information has been received and it is assessed that there is a **substantial** threat to government targets within a specified period of time. This Alert State could be adopted as a general or local warning and would normally be applied for a limited period only. The date for review will be set at the time of rise to BIKINI AMBER.

6. **BIKINI RED.** A specific threat or other definite information indicates that an **imminent** terrorist attack against a particular government target or in a particular area can be expected; or an object, suspected to be a bomb, has been found. This Alert State would normally only be applied as a local warning and for a very limited period.

[1] The same Alert State definitions and associated colour codes apply to the BFG KEENWIND system used in Germany, Belgium, France and the Netherlands.

This page intentionally left blank

APPENDIX 1 TO ANNEX A TO SECTION III TO CHAPTER 7

MOD BIKINI WHITE ALERT STATE - COUNTER MEASURES

W1. **Incremental Action.** WHITE Alert State is the first and lowest of the five Counter-Terrorist Alert States. Together with the Counter-Terrorist Baseline measures, it provides the foundation of countermeasures on which the other Alert States are based. All of the following countermeasures, which constitute good security practice, are to be implemented.

W2. **Review of Security Procedures and Preparation of Contingency Plans.**

a. Regularly review and where necessary update all relevant contingency plans and security instructions. These should include the Counter-Terrorist Alert State System, threat assessment and dissemination, warning and Alert State systems and reporting of terrorist-related incidents, physical defences, orders for guards and patrols, security of vulnerable areas and events, contingency planning and post-incident reporting, action in the event of a terrorist attack, local vigilance schemes, personal security and travel security. In buildings where there are more than one occupier, all parties should be encouraged to participate in the process.

b. Identify buildings, and areas and other locations within the establishment, where personnel congregate and which might be vulnerable to improvised explosive device (IED), vehicle borne IED (VBIED) or mortar attack.

c. Make plans for protective security measures around particularly vulnerable and/or attractive targets.

d. Basic building protection measures should be reviewed and works service action initiated for protective security measures around particularly vulnerable and/or attractive targets, especially with respect to the use of anti-shatter film/curtains in buildings normally housing a large number of personnel. Review the scope for any immediate self-help protective works to lessen vulnerability to IED, VBIED or mortar attack.

e. In consultation with the Police, review the area around establishments to identify areas vulnerable to terrorist attack. This should include locations where large VBIEDs (LVBIEDs) could be parked and also mortar firing points. Agree contingency plans to overcome any vulnerabilities.

W3. **Personal Security.**

a. Brief all personnel, at least annually, to be alert, suspicious and vigilant, especially concerning strangers, unknown vehicles, unattended packages and articles, and suspect postal packages. The brief should also advise personnel on the correct action to take.

b. Where appropriate, advise personnel to adopt those measures which protect information or practices the compromise of which could not be reversed or countered in the event of an increase in the threat.

c. Brief personnel on the principles of anonymity and advise them to adopt those countermeasures which protect personal information or routines.

W4. **Security Measures at Establishments.**

a. Positively identify all persons entering establishments, including staff, visitors and contractors.

b. Carry out periodic security patrols.

c. Ensure that perimeter walls/fences are in good repair. Where appropriate, all unnecessary undergrowth on departmental land concealing both approaches to the perimeter and potential mortar firing points should be removed.

d. Maintain a clear and tidy area in and around all buildings so that unusual packages or articles can be spotted easily. If possible, consider moving objects (e.g. dustbins and crates) which could be used to hide an explosive device to at least 25 metres away from occupied buildings, or keeping them in a secured or supervised building.

e. Ensure that fire fighting equipment is well maintained and that drills are practised.

f. At least annually, hold practice bomb alerts and rehearse action on the discovery of a suspected IED, VBIED or mortar attack, and for dealing with suspect delivered/postal devices.

g. Escort visitors as necessary.

W5. **Travel Security.** Departmental vehicles should be locked when left unattended.

APPENDIX 2 TO ANNEX A TO SECTION III TO CHAPTER 7

MOD BIKINI BLACK ALERT STATE - COUNTER MEASURES

B1. **Incremental Action.** Implement all security arrangements applicable to BIKINI WHITE and in addition, the measures detailed below. BIKINI BLACK is the lowest Alert State at which the MOD will consider the arming of MOD guards and sentries.

B2. **Review of Security Procedures and Preparation of Contingency Plans.**

a. Arrange for the Duty Officer to be on call, preferably by telephone, and to be prepared to initiate additional security plans at short notice.

b. Review plans for controlling vehicle access to establishments.

c. Inform the appropriate Security Authorities and civil police in advance of any Service events planned to be held in public places and also of any major events on MOD property to which the public has access in accordance with the requirements for Public Military Events.

d. Ensure that security works service action initiated under BIKINI WHITE have been completed. If not, consider the implementation of low cost physical protective measures.

B3. **Personal Security.**

a. Brief all personnel on the change to the Alert State.

b. Brief all personnel to increase their vigilance. The whole establishment must be seen to be alert to the threat. Particular attention is to be paid to the briefing of security patrols, guards, sentries and watchmen or caretakers.

c. Brief all personnel on the need to pay particular attention to checking vehicles, including private vehicles, after they have been left unattended.

B4. **Security Measures at Establishments.**

a. Carry out periodic security patrols and sweeps.

b. Limit the number of access points for vehicles and pedestrians. Consider using other exits on a random basis.

c. Make spot checks of parked vehicles.

d. Where appropriate, keep external lighting on at night.

e. Wherever possible prevent vehicles from parking within 25 metres of occupied buildings.

f. Institute random patrolling by establishment security personnel or civil police as appropriate in areas where potential mortar firing points and possible IED and VBIED locations cannot be adequately observed from existing guard positions or using CCTV at main guardrooms or security control rooms. These patrols should be made at irregular intervals and without warning so that this measure cannot be predicted by a terrorist, thereby denying the terrorist the opportunity to avoid the counter measure.

g. At least once every six months, hold practice bomb alerts and rehearse action on the discovery of a suspected IED, VBIED or mortar attack, and for dealing with suspect delivered or postal devices.

h. Escort visitors as necessary.

B5. **Travel Security.**

a. Regularly check travel arrangements to ensure that coaches and passenger carrying vehicles are searched before use, are not left unattended and that all passengers and baggage are carefully checked. Collection and disembarkation points should be on protected property, wherever possible.

b. Drivers are to be briefed about the threat and the measures they should adopt to counter terrorist attacks.

c. Review measures for safeguarding Service transport, particularly when parked in public places.

APPENDIX 3 TO ANNEX A TO SECTION III TO CHAPTER 7

MOD BIKINI BLACK SPECIAL ALERT STATE - COUNTER MEASURES

BS1. **Incremental Action.** Implement all security arrangements applicable to BIKINI BLACK and, in addition, the measures detailed below.

BS2. **Review of Security Procedures and Preparation of Contingency Plans.**

a. Confirm that the civil police are aware of the increased Alert State and co-ordinate security measures where appropriate.

b. Ensure that additional guards can be made available at short notice.

BS3. **Personal Security.**

a. Brief all personnel on the change to the Alert State.

b. Brief all personnel on the increased threat to security and advise them of appropriate personal security measures. Ensure that all personnel are, or have been, briefed on the plans and instructions for action to be taken in the event of a terrorist attack; particularly in respect of IED, VBIED or mortar attack. NOTE: A thorough knowledge of the action to be taken is essential if casualties are to be minimized.

c. Regularly examine routine patterns of activity and where possible modify them to avoid presenting a predictable target.

d. Implement, in consultation with the civil police as necessary, precautionary measures at public places of entertainment frequented by Service personnel.

e. Implement SHARKWATCH for groups of MOD personnel on or off duty, particularly at places of entertainment. One member of the group to be nominated as look-out on behalf of the remainder.

BS4. **Security Measures at Establishments**

a. If possible, move objects (e.g. dustbins and crates) that could be used to hide an explosive device to at least 25 metres away from occupied buildings, or keep them in secured or supervised buildings.

b. Inspect the exterior and interior of all buildings prior to occupation at least daily. Where applicable, particular attention should be paid to domestic

accommodation and general purpose areas (e.g. recreation and dining areas) that may require more frequent searching. Buildings, rooms and cupboards not in regular use should be searched and secured, and then inspected periodically.

c. Further reduce the number of access points as far as possible by erecting physical barriers. Establish check points at all entrances remaining in use. Conduct random searches of vehicles and hand baggage of any person about whom there is any suspicion and delay entry until their bonafide is confirmed.

d. Increase the frequency of security patrols and sweeps within perimeters.

e. Carry out regular checks of perimeters and areas adjacent to them. Whenever possible this should be done in conjunction with the civil police.

f. Pay particular attention to the checking of goods being delivered to stores, restaurants, living accommodation etc.

g. Using establishment resources, if available and as appropriate, and in consultation with the civil police, monitor potential mortar firing points and possible IED or VBIED positions.

h. Institute security checks at entrances to museums and other similar places open to the general public.

i. Escort visitors as necessary.

j. Check all sites not normally occupied by MOD personnel prior to use or occupation. (The term sites includes ranges, assault courses, training camps, sports grounds, drill halls etc).

BS5. **Travel Security.**

a. Wherever possible vary routine timings, particularly for passenger journeys.

b. When not in a protected area safeguard all departmental transport.

c. Ensure that collection and disembarkation points associated with coach travel arrangements are varied or are on protected departmental property and that routes are varied wherever possible.

APPENDIX 4 TO ANNEX A TO SECTION III TO CHAPTER 7

MOD BIKINI AMBER ALERT STATE – COUNTER MEASURES

A1. **Incremental Action.** Implement all security arrangements applicable to BIKINI BLACK and BIKINI BLACK SPECIAL and, in addition, the measures detailed below.

A2. **Review of Security Procedures.**

a. Confirm that the civil police are aware of the increased Alert State and consult them about precautionary measures to be taken outside perimeters.

b. Confirm that all personnel with regular access to establishments considered to be at risk have been briefed on the action to be taken in the event of a terrorist attack; particular mention should be made of the action to be taken for IED, VBIED or mortar attack.

c. Where appropriate, cancel activities that might place MOD personnel at risk other than those that are essential.

A3. **Personal Security.**

a. Brief all personnel on the change to the Alert State.

b. Brief all personnel of the increased threat and draw attention to the importance of applying their personal security measures.

A4. **Security Measures at Establishments.**

a. Increase strength of guard if necessary.

b. Where applicable, erect ramps or chicanes to control the speed of vehicles.

c. Search as many vehicles, briefcases and packages being brought into establishments as possible.

d. Enforce very strict control of access. Reduce to the minimum and, where practical, deny access to the establishment to non-departmental personnel.

e. Implement establishment and civil police contingency plans for frequent patrols of vulnerable areas to enhance security and to deter the use of potential mortar firing points, IED and VBIED locations.

f. Where necessary take additional protective security measures at particularly attractive targets.

g. Prevent vehicles from parking within 25 metres of all occupied buildings.

h. Increase the frequency of searches of parked vehicles and of buildings.

i. Reduce to the minimum the use of top floors of frangible buildings that give minimum protection.

A5. **Travel Security.**

a. When not in a protected area guard departmental transport wherever possible. If vehicles are left unattended, they are to be searched thoroughly before use.

APPENDIX 5 TO ANNEX A TO SECTION III TO CHAPTER 7

MOD BIKINI RED ALERT STATE – COUNTER MEASURES

R1. **Incremental Action.** Implement all security measures applicable to Alert States BIKINI AMBER and, in addition, the measures detailed below.

R2. **Review of Security Procedures.**

a. Confirm that the civil police are aware of the increased Alert State and consult them with a view to their closing public roads that might otherwise make establishments particularly vulnerable to terrorist attack.

b. Consider closing MOD controlled roads to the public.

c. Cancel all activities that might place Service personnel at risk other than those that are operationally or administratively essential.

R3. **Personal Security.**

a. Brief all personnel on the change to the Alert State.

b. Brief all personnel about the very high threat.

c. Do not permit personnel to congregate in large groups.

R4. **Security Measures at Establishments.**

a. Ensure that the strength of the guard force is such that the establishment presents a very secure posture.

b. Search all vehicles, briefcases and packages being brought into establishments.

c. Search all parked vehicles immediately the RED Alert State is imposed and at more frequent intervals thereafter.

d. Deploy resources, if available, in conjunction with the civil police and MDP as appropriate to deny the use of potential mortar firing points, IED and VBIED to terrorists.

e. According to the nature of the threat, review and adjust where necessary, the concentrations and locations of personnel, inside and outside establishments, in order to reduce the risks to them.

f. Avoid, wherever feasible, the use of single storey buildings and the top floors of accommodation blocks.

g. Equip guards at appropriate locations with alarms so that they can give warning of any mortar, IED or VBIED attack.

h. Institute patrols around Service families accommodation areas consulting, where appropriate with the civil police.

i. Review security arrangements of personnel living in Substitute Service Single Accommodation and Substitute Service Families Accommodation.

R1. **Travel Security.**

a. Search and guard department vehicles that need to be used outside establishments.

ANNEX B TO SECTION III TO CHAPTER 7

MOD TESSERAL ALERT STATES – DEFINITIONS

1. **TESSERAL BLACK.** TESSERAL BLACK is a general warning of possible terrorist attack against aircraft by extremists armed with man-portable SAM or AAMG without any particular target being defined. This Alert State is the minimum to be applied while Irish republican and other terrorist organizations are assessed as posing an active threat to aircraft by SAM or AAMG attack in Great Britain (GB).

2. **TESSERAL BLACK SPECIAL.** TESSERAL BLACK SPECIAL is issued as a general warning that there is an increased likelihood of extremists armed with man-portable SAM or AAMG attacking an aircraft at an unspecified location in GB.

3. **TESSERAL AMBER.** TESSERAL AMBER is issued as a warning that extremists armed with man-portable SAM or AAMG intend to attack an aircraft in GB in the near future. It could be issued as a general or local warning and would normally be applied for a limited period only.

4. **TESSERAL RED.** TESSERAL RED is issued as a warning that an attack against an aircraft in GB by extremists armed with man-portable SAM or AAMG is imminent. It will normally only be issued as a local warning and for a very limited period.

This page intentionally left blank

APPENDIX 1 TO ANNEX B TO SECTION III TO CHAPTER 7

MOD TESSERAL ALERT STATES – COUNTER MEASURES

Preparatory Measures

1. The preparatory measures listed below are to be reviewed periodically by units and establishments and details reported through the chain of command.

a. **Appreciation and planning - Commands and HQ**. Commands and HQ are to review the vulnerability of and risk to establishments and, as appropriate, order the implementation of preparatory measures.

b. **Appreciation and planning - establishments**.

(1) If ordered, a reconnaissance is to be carried out and an appreciation made to identify likely firing points taking into account the maximum assessed altitude and the maximum range of the SA7B and AAMGs in relation to the take off and landing patterns practised at the airfield or helicopter landing site (HLS). (see Note 3).

(2) Contingency plans are to be made and orders and instructions drafted for action to be taken at TESSERAL Alert States or in the event of a terrorist SAM or AAMG attack. Detailed orders and instructions will vary between establishments to take account of the type of aircraft operated and local factors.

c. **Briefing and liaison.** Establishments are to liaise with their local civil police and MDP as appropriate, in order to agree with them on local TESSERAL plans and counter measures and to seek their advice and assistance.

TESSERAL BLACK

2. Review and update, where necessary, all the contingency plans, orders and instructions relating to TESSERAL and implement the following additional counter measures:

a. **Briefing.** Brief all personnel (Service and civilian) on the threat and the orders and instructions for higher TESSERAL Alert States.

b. **Liaison.** Establishments are to liaise with their local civil police, and MDP as appropriate, in order to brief them on local TESSERAL plans and counter measures and to seek their advice and assistance.

TESSERAL BLACK SPECIAL

3. Review all the actions carried out at TESSERAL BLACK and implement the following additional counter measures where appropriate:

a. **Briefing and liaison**.

(1) Brief all personnel of the increased threat, especially pilots, ground support crews and aircraft controllers.

(2) Inform civil police of the threat and co-ordinate plans for safeguarding aircraft flight paths into and out of establishments.

(3) Prepare to activate contingency plans, and issue detailed Air Traffic Control (ATC) procedures.

(4) Be prepared to receive and direct aircraft from other establishments.

b. **Precautions inside establishments**.

(1) Institute patrols to search areas within MOD establishments' perimeters from which attacks on aircraft could be made and take action to ensure that no extremists armed with a SAM or AAMG can operate against aircraft from within the perimeter.

(2) Hold practice alerts within establishment perimeters.

c. **Precautions outside establishments**.

(1) In conjunction with local civil police carry out regular checks of perimeters, especially under and adjacent to flight paths.

(2) Remind the civil police of any areas outside the perimeter from where attacks could be mounted and that cannot be avoided by aircraft on take off or landing.

(3) Warn all aircrew to report any unusual activity seen near approach and overshoot areas.

TESSERAL AMBER

4. Implement all security arrangements applicable to TESSERAL BLACK SPECIAL and implement the following additional measures where appropriate:

a. **Briefings and liaison**.

(1) Brief all personnel of the increased threat.

(2) Inform local civil police of the increased threat and consult them on precautionary measures to be taken outside establishments' perimeters.

(3) Implement appropriate flying counter measures laid down in SOPs, as directed by ATC.

b. **Precautions inside establishments**.

(1) Increase patrols within perimeters and maintain continuous observation of approach and overshoot areas.

(2) Reduce flying to essential operational flights only and cease circuit flying.

(3) Close relief landing grounds.

(4) Check airfield diversion state.

c. **Precautions outside establishments.** Establishments are to be prepared to react to requests from Command HQ to provide Service personnel to assist the civil police to search the approaches outside the perimeter of Service airfields for terrorists under normal Military Aid to Civil Power (MACP). [See Notes 1 and 2]

TESSERAL RED

5. Review all security arrangements applicable to TESSERAL AMBER and implement the following additional measures where appropriate:

a. **Briefing and liaison**.

(1) Brief all personnel of the very high level of threat.

(2) Inform local civil police of the increased threat.

b. **Precautions inside establishments**.

(1) Cease all flying except for specifically authorized operational sorties and implement appropriate flying counter measures.

(2) Be prepared to accept aircraft diverted from other establishments.

(3) Be prepared to deploy light aircraft and helicopters for surveillance tasks (against SAM only - not in the event of an AAMG threat).

c. **Precautions outside establishments.** Consider closing military roads allowing access to the airhead.

Notes:

1. Normally action outside MOD establishments will be entirely a matter for the Chief Police Officer who, on receipt of a TESSERAL alert will take whatever action considered appropriate. Exceptionally, and after consultation with the Home Office, the Chief Police Officer may request aid in:

   a. Providing deterrent patrols in the area around airfields.

   b. Helping to deal with terrorists who have been located but, because of their actions or the way they are armed, are beyond the power of the civil police to handle.

2. Any assistance given by the Services outside the perimeters of MOD establishments will come under MACP and will always be at the request of the civil police. Any request for or provision of such assistance should be reported as soon as possible through the chain of command.

3. Detailed characteristics of man-portable SAMs and AAMGs which are likely to be in the possession of terrorist have been issued by the MOD to PSyAs and Command security staff. ESyOs responsible for the implementation of TESSERAL counter measures should ensure that they have access to this information.

ANNEX C TO SECTION III TO CHAPTER 7

GUIDANCE ON MORTAR ATTACK COUNTER MEASURES - ORDERS AND INSTRUCTIONS

Introduction

1. The guidance set out below will probably need to be addressed in any orders or instructions produced by individual establishments concerning the planning, briefing and action to be taken before, during and after any terrorist mortar attack. The guidance given is not exhaustive and should be applied with due regard to the local circumstances applicable to a particular establishment. Thought should be given to consulting local civil police and other Service agencies that may be able to give professional advice on the application of mortar counter measures and their implementation.

Preparation

2. A standard mortar attack alarm and all clear signal equipment must be immediately available to guards and easily identifiable as such by personnel within an establishment.

Immediate Action in the Event of an Attack

3. The mortar attack alarm must be sounded immediately an attack is suspected.

4. On hearing the attack alarm, the sound of a mortar firing, or the detonation of a mortar round, all personnel are to take cover immediately by:

a. **Inside buildings.** Lying on the floor or ground. Where possible, this should be done away from windows and preferably under some form of shelter such as tables, beds, desks or in internal corridors. (Some buildings may have pre-designated bomb shelter areas).

b. **Outside buildings.** Seeking cover immediately wherever they can, and then moving as quickly as possible to the shelter of a building as soon as the alarm or explosions stop.

c. **Vehicles.** Vehicles should not be abandoned obstructing roads.

5. Guards should take cover in guard posts where available and close viewing ports if fitted. Guards should count the number of reports from the baseplate, the general direction from which the mortar(s) firing is coming and the reports of the bombs exploding. These details are then to be relayed to the main guardroom or security control room.

6. Personnel should remain under cover unless:

a. They are ordered to move.

b. They are aware of an unexploded bomb nearby.

c. They are aware of a casualty requiring assistance.

d. The all clear sounds.

7. Personnel who are aware of the existence of an unexploded missile or casualties are to inform the security control room or ICP immediately.

8. The security control room is to inform the civil police, the superior HQ and the focal point system of the attack. The assistance of an EOD officer is to be requested by the establishment or civil police and an RVP arranged away from the establishment.

Action by the HOE

9. As each attack will probably be different, there is no standard time for personnel to remain under cover. Much will depend on the number of mortars believed to have been used, as the likelihood of unexploded or non-fired bombs increases with the greater number of mortars used in the attack and therefore the longer personnel should remain protected. Those in charge will have to make their own judgement at the time.

10. Once the establishment has been secured and any casualties dealt with, the clearance of the base plate position and any unexploded bombs should follow the normal procedures for dealing with IEDs. This procedure should include clearance of the area, the establishment of a cordon and an ICP by the civil police. The HOE is to act in support of and as requested by the civil police, keeping his own authorities informed.

11. Once the base plate has been located, the area around the baseplate, the area under the flight path and the impact area must all be cleared of personnel and cordoned off. The evacuation of the area under the flight path is essential in order to minimize the danger from an unfired or delayed action bomb still remaining in a mortar. These requirements may entail the complete evacuation of the establishment.

12. Orders and instructions should include measures to cope with the disruption caused by the attack to mains power and communication facilities and the potential risks involved with hazardous or inflammable materials within the establishment.

13. The all clear should not be given until the ATO and the civil police commander agree that it is safe to re-enter the cleared area.

ANNEX D TO SECTION III TO CHAPTER 7

THE ISSUE AND USE OF BATONS BY SERVICE PERSONNEL

Introduction

1. A baton is a weapon that has the capability to seriously injure or kill. It is therefore essential that those using a baton are authorized to carry it, are correctly trained in its use and understand the circumstances that will allow its use. For the purpose of this paper the term 'baton' includes any truncheon (generally regarded as obsolete), expandable baton or rigid baton specifically designed for an operational, security or policing purpose. It should not be confused with 'baton rounds', used in public order situations, for which separate instructions apply. The use of pickhelves, staves or any other implement as a substitute for a purpose-designed baton is not authorized.

Aim

2. The aim of this paper is to outline the situations in which the use of batons by Service personnel may be authorized, and the procedures and constraints that apply to their issue and use.

The Requirement for Batons

3. A number of situations are envisaged when batons may be required. These may be operational, security or police related. The provision of a baton will allow a graduated response, from an unarmed reaction through to the use of a firearm, if issued, depending on the situation and the ROE in force.

4. Batons may be a suitable weapon for use in both Peacetime Operations and during Armed Conflict. The requirement for batons will therefore vary depending on the nature of the conflict at the time.

5. The list of circumstances that follows illustrates the range of situations for which the issue of batons may be appropriate.

Operations

6. Members of the Armed Forces may require to use batons in order to achieve a mission on any type of Military Operation within the Spectrum of Conflict. Within such an operation, batons may provide an effective option to, or be used with, other weapons.

7. Examples of such Military Operations include:

a. Public Order operations within military aid to the Civil Power.

b. Peacekeeping or Peace Enforcement Operations.

c. Military Home Defence.

d. Non-combatant Evacuation Operations.

Security

8. In order to provide security for the Department, personnel may be posted as sentries to guard property or personnel. The MOD has a responsibility to equip its personnel for the task on which they are employed and therefore a sentry should be equipped on a basis commensurate with the assessed threat. A sentry could therefore be equipped with a firearm (and perhaps also a baton), with a baton, or unarmed.

Policing Duties

9. The MDP and Service Police require batons to execute Police Duties. Where their use has been approved by Minister (AF), CCMDP and Service Police Provost Marshals will issue separate police instructions which accord with the Association of Chief Police Officers (ACPO) guidelines. Consequently, this Policy Paper does not apply to the MDP and/or the Service Police.

10. Batons could be required by Service personnel who may not be Service Police but who could be employed in support of Service Police e.g. patrols, sentries or in response to a specific incident.

Summary

11. Batons offer an effective weapon to provide:

a. Deterrence through display of capability.

b. Individual protection of the Servicemen or of others from aggressors in a variety of scenarios, and for the protection of property.

c. An offensive capability short of the use of a firearm.

Authority for the Issue of Batons

12. Given that a baton has the capability to kill or seriously injure, with consequences for the individual using a baton and the Department, and in line with arming policy for firearms, approval for their issue must be given at the appropriate level. The issuing of batons for operational use would reflect the policy promulgated in the relevant ROE profile. Ministers have agreed to standing authority being given to CINCs for the issue of batons for security guarding purposes; this authority may be delegated down the respective chains of command. When batons have been issued for security purposes CEAG is to be informed.

13. Trained Personnel. Batons should only be issued to appropriately trained personnel. Planning is to allow for sufficient trained personnel to be available to meet foreseeable scenarios.

14. Self Defence. In extremis, when faced by a particular substantive and immediate threat and where the issue of batons may resolve the immediate situation, Commanding Officers/Heads of Establishments (CO/HOE) and operational commanders may order the issue of batons, notifying the chain of command as soon as possible.

Guidance on the Use of Batons

15. Minimum Force. For all operations at home, and those abroad where host nation consent for operations has been obtained, UK Forces will be under the jurisdiction of English Domestic Law as enshrined by Section 3 of the Criminal Law Act 1967. Thus, minimum force for all operations, other than where the laws of armed conflict apply is defined as:

"A person may use such force as is reasonable in the circumstances in the prevention of crime or in effecting or assisting in the lawful arrest of offenders or suspected offenders or persons unlawfully at large".

16. Further guidance, designed for use in the field, is provided at JSP 398.

Training

Requirements

17. Those issued with a baton have the option to respond by means of overt deterrence at the lower end of the scale, up to use of potentially lethal force at the other. It is necessary therefore to ensure that all personnel equipped with a baton have confidence in their ability to use it correctly in a number of situations within the law.

18. Training to meet Single Service requirements is necessary and it is for Single Services to decide how these requirements are to be met incorporating the guidelines and training objectives at Annex A. The training is to ensure that the trainee understands how to use the baton correctly in a number of scenarios and this will help fulfil the MOD's responsibilities as an employer.

Records of Training

19. A clear and auditable record of initial and continuation baton training carried out by Service personnel is to be maintained and available for scrutiny when required.

Resource Implications

20. Provision of Batons. The provision of batons, if required, will be a Single Service responsibility. Only batons, as defined in paragraph 1, are to be issued and any other implements currently issued for use are to be withdrawn.

21. Training Costs. Training costs are to be met by the Single Services.

Conclusions

22. The following conclusions have been reached:

a. Batons may be required for the protection of MOD personnel and property in a number of situations (para 3).

b. Authority to issue batons for operational use will reflect guidance articulated in the relevant ROE profile (para 12).

c. Standing authority is granted to CINCs to issue batons for security guarding purposes (paragraph 12).

d. Batons should only be issued to appropriately trained personnel (para 13).

e. Guidance for the operational use of batons at home and abroad, short of Armed Conflict, is to be in accordance with English domestic law (paragraph 15).

f. Single Services are responsible for determining the scale of the training requirement and for the implementation of suitable training (para 18).

g. Auditable records of training are to be kept (para 19).

h. Training and procurement costs will lie where they fall (paragraphs 20 and 21).

APPENDIX 1 TO ANNEX D TO SECTION III TO CHAPTER 7

BATON TRAINING

General Guidelines

1. The following points relate to all personnel undergoing baton training.

   a. A safety brief must be given as part of the introduction.

   b. All personnel must qualify on the basic course before being armed with the baton.

Training Objectives (Applicable to all Types of Batons)

2. At the conclusion of the course the student must be able:

   a. To explain the nomenclature of a baton.

   b. To demonstrate a clear understanding of the use of minimum force.

   c. To perform all practical baton techniques and associated movements effectively.

   d. To demonstrate a clear understanding of the baton ROE and their use in all relevant scenarios. (To achieve this, Home Office Police Forces and the RN use the 'Conflict Resolution Model' as a basis for their training).

   (Experience gained by Police forces and the RN has shown that the above elements of training takes a minimum of 4 hours to complete).

This page intentionally left blank

APPENDIX 2 TO ANNEX D TO SECTION III TO CHAPTER 7

ROE FOR THE USE OF BATONS

Guidance for the Use of Batons by Service Personnel

General Rules

1. These ROE do not affect your general right to self-defence. However in all situations you are to use the minimum force necessary to achieve your aim. Your baton may only be used as a last resort.

2. Where personnel are authorized to use Public Order Control Equipment, JSP 398 Card D should be issued.

Challenging and Warning

3. A challenge should be given before using your baton. (A challenge need not be given if to do so would increase the risk of death or injury to you or others, for example because aggressive confrontation is imminent).

4. You are to challenge by shouting:

> *"ATTENTION - STOP/MOVE/DISPERSE* OR I MAY USE A BATON AGAINST YOU" (* As appropriate)*

Striking

5. If you have to strike you should USE THE MINIMUM FORCE NECESSARY TO ACHIEVE YOUR AIM.

Use of Lethal Force

6. Striking in a manner that may cause a fatality constitutes the use of potentially lethal force. You may only strike a person in such a way:

If he/she is committing or about to commit an act

> LIKELY TO ENDANGER LIFE, AND THERE IS NO LESSER WAY TO PREVENT THE DANGER.

After Striking

7. After striking you should:

a. Re-assess the situation;

AND

b. Decide upon any follow-up action required. (e.g. strike again, summon assistance or give first aid).

Protection of Specified Property, Equipment or an Installation

8. This extra paragraph operates ONLY when your superior has told you that it applies to a specified property, installation or equipment that you are guarding. If this paragraph is authorized, then you may use a baton against a person if:

a. He/she attempts to take possession of that specified property, installation or equipment, or to cause it serious damage, which could prevent its effective use, or to destroy it;

AND

b. There is no other way of preventing this;

BUT

c. All other Card E rules apply.

SECTION IV TO CHAPTER 7

COUNTER TERRORIST PROTECTION WITHIN ESTABLISHMENTS AND ELSEWHERE

General

07401. Thorough planning and supervision of protective measures is needed to defeat terrorist attack. It is important to try to foresee what forms of attack terrorists might adopt. In particular, establishments and individuals should assess where they are most vulnerable and concentrate on these areas, instead of attempting to protect everything, to the same extent, all the time. Protective measures stand the best chance of succeeding if:

a. Sound plans exist which are sufficiently simple and flexible to respond quickly to changes in the threat and in the manning state of the establishment.

b. There are clear orders, standing operating procedures (SOPs) and guidance.

c. Everyone is properly educated about the threat, briefed, trained, practised and alert.

Plans

07402. Counter terrorist plans should cover the general precautions required at all times, the action to be taken at each Alert State, and how to react to emergencies. They should be based on command instructions and draw on the guidance given in this Chapter and Chapter 5. They should include such matters as:

a. **External protection and control of access.** This should cover guarding arrangements, the searching of vehicles and people on entry, passes, restrictions on movement where civilians have access to military roads, the security of the establishment perimeter, and observation generally (external and internal).

b. **Internal protection.** This should cover the general state of preparedness of the establishment, including such matters as guard and reaction forces, lighting, parking, searching, building security, medical arrangements, fire fighting, arrangements for the delivery of mail and goods, and escorts for visitors and other similar points relevant to the establishment. Emphasis must be given to the protection of personnel in such places as accommodation blocks, NAAFIs, messes, etc. Plans should be made for the protection of sensitive targets such as armouries, guardrooms, ammunition stores, vehicles, other major equipment, communications centres and telephone exchanges, etc.

c. **The protection of personnel and families when outside the establishment both on and off duty including movement.** Protective arrangements must be included for those soft targets that are not normally protected

but that may be vulnerable in periods of high threat such as Service families accommodation areas (in conjunction with the civil police where appropriate), or other living accommodation, ranges and local training areas, public houses and cafes, transport facilities such as buses and railway stations, etc, regularly used by Service personnel.

d. **Counter measures.** This should cover the measures to be taken in the event of a terrorist attack or other contingencies, including orders for the issue of arms and ammunition.

e. **Liaison.** The arrangements for liaison with the local police and adjacent military establishments should be specified, and their participation reflected in establishment security plans.

f. **Post incident procedures.** These should cover the procedures and actions to be carried out in the event of a terrorist attack.

Orders

07403. Establishment orders, apart from covering the matters at paragraph 07402 above, must give specific guidance on the action required in the event of the following:

a. Changes to the Alert State.

b. A specific threat to the establishment.

c. The discovery of a suspicious item in the mail or other suspicious objects elsewhere, including guidance on the identification of such objects.

d. Any form of evacuation that is necessary.

e. The discovery or suspicion of intruders.

f. Other suspicious activity that may relate to terrorism.

g. An explosion or attack.

h. A mortar attack.

i. Requests for Military Aid to the Civil Power (MACP).

j. Other contingencies.

07404. Additional guidance on matters that should be included in Contingency Planning for Unexpected Events is at Annex A.

Briefing

07405. Establishments must ensure that all personnel are briefed, trained and practised in terrorist precautions. The extent to which this is necessary is for HOE to decide, based on

the current threat, the role and state of training of the establishment and directions issued by superior HQ. A large part of an establishment's protection and that of individuals should be based on the physical security measures described elsewhere in this manual coupled with normal military skills, alertness and initiative. However, there are protective measures that are necessary normally only during periods of high threat; at other times they tend to be forgotten. Advice on such measures is covered in succeeding paragraphs.

Operation ROUNDUP

07406. Operation ROUNDUP is the establishment level operation to alert its personnel to the possible presence of intruders and/or IEDs within the establishment. Its implementation requires:

a. The securing of the establishment.

b. The imposition of rigid control of entry to all areas.

c. The cessation of non-essential movement.

d. The instigation of a thorough search.

07407. All MOD establishments are to have plans to instigate Operation ROUNDUP should the presence of intruders or IEDs be suspected or as a proactive security measure. Focal Point reporting should only be used in the event of an actual terrorist related incident.

Operation WIDEAWAKE

07408. Operation WIDEAWAKE can be used to initiate a search for IEDs at start-work. It can be instigated at establishment level and higher formations can also order its implementation at one or more establishments. Establishments may be passed this codeword, through the Focal Point System, and should consider whether to initiate a similar procedure at their own establishment.

Protection outside MOD Establishments (Less Service Families or Private Accommodation)

07409. Guidance covering aspects of life outside MOD establishments, such as protective measures for drivers, unit movement generally, training, sport, social activities, and travelling arrangements for individuals or groups moving by public or private transport are included at Annex B.

Personal Security at Home

07410. The need for precautions in Service families and in private accommodation will vary widely. Depending on the level of threat, occupants of Service families and private accommodation should either be issued with security advice or briefed on common-sense security precautions. It is not possible to specify precautions to suit all circumstances, but guidance suitable for use by High Threat Personnel (HTP) is given at Annex A to Section V and should be used as the basis for advice for other personnel when the need arises.

Anonymous Telephone Calls or Threats

07411. All personnel in an establishment who are likely to receive anonymous telephone calls or telephone threats directed at the establishment should be briefed on how to react. Officers, NCOs, clerical staff, mess waiters and telephone exchange operators, are among those likely to be affected. Guidance is at Annex C.

Suspicious Letters or Parcels

07412. All MOD personnel should be briefed on how to deal with suspicious envelopes and packages arriving by post. Guidance is at Annex D.

Explosive Devices and Booby Traps.

07413. All MOD personnel should be briefed on how to recognize possible unexploded devices and booby traps and what to do when such devices are suspected or discovered. Guidance is at Annex E.

Searching of Vehicles

07414. Vehicles, both military and civilian, are an easy target for terrorists and all MOD personnel must understand how to search them.

Security at Armed Forces Careers Offices

07415. Experience has shown that Armed Forces Careers Offices and staff are particularly vulnerable to terrorist attack. Located in urban areas, very often in a shopping area with free public access and normally isolated from other Service establishments.

07416. The need to protect careers offices must be balanced with the requirements of Service recruiting policy and the need for an "open door" approach. Security arrangements will also be complicated by local planning restrictions, multiple occupancy of buildings and tenancy or lease agreements. However, the application of the security measures detailed below should provide a realistic degree of security.

The Threat

07417. The types of attack most likely against Armed Forces Careers Offices are as follows:

a. A time delay IED attack close to or inside careers office premises, probably involving the placement of a device in silent hours.

b. A booby trap, postal bomb or similar device delivered to careers office premises.

c. A close quarter shooting against careers personnel arriving, departing or at a careers office. Personnel unlocking and locking premises at predictable times are particularly vulnerable.

d. An under vehicle improvised explosive device (UVIED) attack against a careers office vehicle, particularly if it is clearly identifiable or insecurely parked or parked in a secluded but accessible area.

Security Planning

07418. Each Armed Forces Careers Office must possess a comprehensive security plan that should include the following:

a. Measures for BIKINI Alert States.

b. Briefing and training.

c. Personal security measures.

d. Vehicle security measures.

e. Office security measures.

f. Reporting, to include instructions for reporting terrorist related information to:

(1) Civil police.

(2) Focal Point System contact points.

(3) Normal chain of command.

g. Incident contingency plans, to include:

(1) Immediate response drills.

(2) Evacuation plans.

(3) Search plans.

(4) Joint careers office and civil police post incident plan.

07419. Minimum security standards at Armed Forces Careers Offices are at Annex F.

Briefing and Training.

07420. Provision should be made, as part of induction training for careers offices personnel to receive:

a. Formal security briefings on first arrival and thereafter at regular intervals. These should include coverage of the threat (in particular current terrorist methods of operation), local situation and security orders.

b. Formal security training by specialist staff to cover operational counter measures such as personal security drills and vehicle search.

Immediate Response Drills

07421. Security procedures and immediate response drills, such as office evacuation drills, must be monitored and practised.

Contact Lists

07422. Viable contact lists (24 hour cover) are to be maintained and passed to the relevant Focal Point System node or sub-node and local civil police. This will ensure that careers staff may be contacted at any time.

Security Advice

07423. Careers staff should be encouraged to seek advice from their PSyAs and Command security staff or local security unit. Guidance should also be obtained from current DCIs covering security at public military events and personal security measures.

Contingency Planning and Post Incident Procedures

07424. Operational control and co-ordination of the response to a terrorist incident is the responsibility of the civil police. Each civil police force in GB has drawn up contingency plans to respond to terrorist incidents occurring within their jurisdiction. In most cases, these plans are based upon common terminology and procedures and produced by the ACPO Standing Committee on Emergency Procedures. ACPO emergency procedure terminology is included in the glossary of terms shown at Appendix 1 to Annex G.

07425. HOE are responsible for the immediate action to be taken after a terrorist incident has occurred. Post incident operational control within perimeters is to be handed over to a civil police officer on request. Once a formal hand-over is completed, the HOE is to continue to provide help and support to the civil police as required.

07426. Although the following procedures have been developed for use in GB, the content should be used in overseas commands as a guide to develop local contingency plans.

Contingency Plans

07427. To ensure that correct action is taken by personnel after a terrorist incident has occurred, HOE are to produce written local contingency plans. These plans are to be drawn up in conjunction with the local civil police and should, where possible, be joint plans. To be effective, contingency plans must be regularly rehearsed, ideally with the civil police and other emergency services. Copies of plans should be held by the civil police, other emergency services and appropriate HQ.

07428. The general principles of incident management to be applied at the scene of an incident are detailed at Annex H.

07429. Details of the action to be taken in the event of the terrorist incidents are detailed in the following Annexes and Appendices:

a. Advice on Handling Anonymous Telephone Calls with Warnings or Threats - Annex C.

b. Action upon discovery of a suspect postal bomb - Annex D.

c. Action upon discovery of a suspected IED – Appendix 1 to Annex H.

d. Action should an IED explode – Appendix 2 to Annex H.

e. Action in the event of a mortar attack – Appendix 3 to Annex H.

f. Action in the event of a terrorist shooting attack – Appendix 4 to Annex H.

g. Action in the event of a proxy bomb attack – Appendix 5 to Annex H.

Civil Police

07430. Details of the civil police civil police control and co-ordination of the emergency services' response in the event of a major terrorist incident are at Annex G.

Deployment of Supporting Service Agencies

07431. A number of supporting Service agencies are available to the civil police and establishment to provide post incident assistance if required.

a. **EOD.** Service EOD teams provide assistance to the civil police throughout GB on request. Such assistance is requested by the civil police direct to the JSEODOC at Didcot.

b. **Royal Engineer Specialist Search**

(1) 33 Engr Regt provide specialist search assistance to civil police throughout GB on request.

(2) Any civil police request for specialist search assistance should be passed to Joint Service EOD Operations Centre (JSEODOC).

c. **Helicopters.** Requests for helicopter support should be passed to Command HQ and must be accompanied by full details of the task as follows:

(1) Contact name and telephone number of the person who can give additional details of the task.

(2) Outline details of the task, i.e. Recce, CASEVAC, etc.

(3) Number of PAX to be carried.

(4) Pick-up point and destination.

(5) Communication details.

(6) Timings.

d. **Photo recce.** Photo recce requests are to passed to MOD through the chain of command.

e. **Service police.** Service police will attend the scene of a terrorist incident, and are trained and equipped to provide the following assistance to the civil police:

(1) Cordon and control personnel.

(2) Communications.

(3) Collection, collation and provision of evidence.

(4) Investigation within the local community.

(5) Provision of swift and accurate details of the incident.

(6) Provision of an officer to act as civil police liaison officer if required.

Service Attendance at the Scene of an Incident

07432.

a. Service attendance at the scene of an incident should be restricted to those individuals with a legitimate and defined role to play in post incident action.

b. There is a tendency for uninvited Service representatives to arrive at the scene of an incident to gain information, conduct liaison or speculate. The following is a guide to those persons who should be in attendance:

(1) HOE.

(2) Establishment personnel directly supporting the civil police.

(3) Emergency services.

(4) Specialist personnel such as EOD and local security unit.

Post Incident Information Gathering and Reporting.

07433.

a. There is a requirement following a terrorist incident for swift, accurate information gathering and reporting through the chain of command. Information is required to:

(1) Take action to save life or prevent further loss of life.

(2) Make decisions based upon facts, including the possible changing of security Alert States and the introduction of enhanced security measures.

(3) Identify lessons for the future.

b. The following have information gathering and reporting responsibilities after a terrorist incident:

(1) **Establishment.** Gather immediate post incident information and send Incident Reports to the civil police, and superior formation HQ.

(2) **Security Unit.**

(a) Ensure that D Def Sy, PSyAs and Command security staffs are aware of the incident.

(b) Gather post incident information and within 12 hours of an incident submit a written initial incident report to PSyAs and Command security staffs and to D Def Sy (and RAF only, to HQ RAF P&SS).

(c) Liaise closely with all other appropriate agencies in the compilation of the initial incident report.

(d) Contribute to the compilation of any subsequent reports.

(e) Conduct investigations in support of the civil police.

Media Liaison and Public Information

07434.

a. The civil police are directly responsible for media liaison after a terrorist incident.

b. Establishment responsibilities are as follows:

(1) Provide an update briefing for the Command Media Ops staff who may deploy to the scene of a terrorist incident.

(2) Keep the media away from the scene until media liaison facilities are agreed by the civil police.

(3) The HOE is to be available to broadcast interviews as advised by the Command Media Ops staff or civil police press liaison officer.

(4) The HOE is to avoid comment on security arrangements and is to take steps to ensure that personnel under his command observe similar discretion, even when talking to relatives or acquaintances.

(5) The HOE should bear in mind that public relations is a command function, and that although operational tasks take priority the need to reassure the public or to gain recognition for positive actions taken are significant considerations and in certain circumstances may be of overriding importance.

Security Vigilance Areas (SVA)

07435. An SVA is primarily defined as the ground outside the perimeter from which a MOD establishment or Service families accommodation estate could be observed or attacked by a terrorist group. The size of an SVA will vary, depending upon the local geography. It may also be appropriate to include other locations where personnel are required to congregate and where the setting of routines is unavoidable, e.g. railway stations at particular times.

07436. The setting of an SVA is a local arrangement between the HOE and the local civil police commander; they will determine its boundaries according to local circumstances, availability of resources and counter terrorist security requirements.

07437. It is currently assessed that a terrorist group will normally spend considerable time reconnoitring and making its preparations prior to mounting an attack. One or more members of the group may well be within an SVA watching a target prior to attack. The terrorist group will subsequently enter the SVA to attack an establishment and may select mortar base plates or firing points within the SVA.

07438. It is within the SVA, particularly during the reconnaissance and preparatory stages of an attack, that the terrorist is vulnerable to identification. However skilfully he or she merges into the local pattern of life, the terrorist is usually a stranger in an unfamiliar environment. It is this vulnerability which SVA plans should seek to exploit.

Aim of an SVA

07439. The aim of an SVA is to establish an area, primarily around the outside of establishments, in which counter terrorist security awareness is raised. Joint civil police and MOD measures utilising increased public awareness of the terrorist threat and modus operandi are implemented, if appropriate, to identify suspicious activity and subsequently to deter, disrupt or respond to an attack.

07440. The aim is not one of general deterrence, but one of fully utilising the eyes and ears of those in the vicinity of Service establishments with a view to identifying suspicious activity and reporting it to the appropriate authorities. Publicity of the scheme is to be strictly limited to those living within the SVA.

SVA Plans

07441. SVA plans should include the following:

a. A civil police led observation and reporting plan designed to raise the level of public awareness and identify suspect terrorist activity within the SVA.

b. A civil police led plan designed to respond to reports of suspect terrorist activity within or beyond the SVA.

c. A joint civil police and establishment contingency plan to respond to a terrorist attack.

Implementation of SVA

07442. Phase One - Preparatory Measures

a. **Joint police and Service liaison.** Establishments, in consultation with their PSyAs and Command security staff and civil police HQ, should identify where SVAs are needed and decide whether their satellite establishments need separate SVAs. At locations where other Service establishments are collocated or in close proximity, HOEs should consider establishing joint SVAs. SVA co-ordinating groups may be necessary and could include:

(1) Civil police commanders.

(2) HOE.

(3) ESyO.

(4) Command representative.

b. **Joint police and Service planning.** Once liaison is established the following planning should take place:

(1) A joint appreciation conducted by the local civil police and MOD, to include the following:

(a) Ground analysis to identify potential terrorist approach and escape routes, drop off and getaway rendezvous points, vantage points for terrorist observation and potential firing and mortar base plates points. HOE should take account of any previous action resulting in security or counter terrorist surveys that could provide much of the information needed.

(b) An assessment of establishment vulnerability and identification of potential targets, e.g. accommodation blocks, messes and main guardroom.

(c) A pattern-of-life study to establish what is normal within an SVA, e.g. local routines, local vehicles, etc (identifying normality is a precursor to spotting the abnormal).

(d) An assessment of civil police and MOD resources available to implement an SVA plan.

(2) **Production of SVA plan.** The SVA plan should include:

(a) Map showing SVA boundaries.

(b) Observation and reporting arrangements.

(c) Operational response to reports of suspected terrorist activity.

(3) **Education and training.** The key to the possible identification of suspect terrorist activity within an SVA is likely to be appropriate education within the civil police, the establishment and the local civilian community.

(a) Within the civil police and Services, education and training might include terrorist methods of operation, familiarity with the ground, the SVA pattern of life, observation and reporting techniques, vehicle recognition and joint police and Service incident handling drills.

(b) Within the local civilian community, increasing the level of awareness of the terrorist threat and modus operandi may require publicity material, follow up visits by the civil police and possibly the involvement of neighbourhood watch committees.

07443. Phase Two - Implementation of the Observation Framework

a. **Civilian Involvement.** Distribution, normally under civil police arrangements, to all dwellings and shops throughout the SVA of the publicity material produced by MOD.

b. **Civil Police.** Chief Constables to decide upon the appropriate deployment of foot and vehicle patrols in uniform and civilian clothes within an SVA in light of the local needs and circumstances.

c. **Service Personnel**

(1) **On duty.** Observation from establishment perimeter vantage points into the SVA conducted by Service guards, MGS, Service Police or MDP.

(2) **Off duty.** Observation and awareness by all Service personnel, dependants and civilian employees as they pass through the SVA.

(3) **At home.** Encouragement to become involved in neighbourhood watch schemes, both as participants and co-ordinators.

07444. Phase Three - Implementation of Local Information Reporting System

a. **Reporting system.**

(1) **Civilians.** Directly to the local civil police using the 999 system or a locally arranged Freephone system.

(2) **Civil police.** By radio or report directly to the civil police control room.

(3) **Service personnel.** Either directly to the civil police or where this has been agreed locally, to the main guardroom or Service police.

(4) **Establishments.** Where information is passed other than to the civil police, in the first instance, establishments are to ensure that it is relayed immediately to them. All reports are also to be passed to the local MDP or Service police unit and to the OP MARSHALL Cell within 2 MI Bn as appropriate.

b. **Collection system.** The civil police are responsible for the handling of all terrorist related information produced within the SVA. However, various Service police and security agencies have collation systems for all security reports passed to them including those related to SVAs. Such reports are then passed on to the civil police and other agencies as appropriate.

Maintenance of SVAs

07445. Security is, in part, an attitude of mind and is a continuous process. The local civil police commander and HOE will need to consider appropriate means of maintaining security awareness through repetition and reinforcement of the need to maintain vigilance. This could include:

a. A civil police led additional leafleting programme.

b. Inclusion in new arrival briefings, periodic security education and repeat routine orders.

Plan to Respond to Reports of Suspicious Activity

07446. As a corollary to the establishment of SVAs, HOEs will need to prepare and maintain contingency plans, in conjunction with the civil police, for activation in the event of reports of likely terrorist activity:

a. Within the SVA, the response to a report of suspicious activity is likely to be an exclusive civil police operation.

b. The operational response of the civil police within an SVA is likely to be mirrored by an appropriate response within the perimeter of an establishment.

Joint Contingency Plan in Response to a Terrorist Attack

07447. The HOE in conjunction with the civil police, is to produce contingency plans covering the eventuality of a terrorist attack and the likely response to it.

Security at Public Military Events

Definition

07448. A Public Military Event (PME) is an event that the Services organize or participate in, about which the general public has prior knowledge and to which they have access. The term includes civil events with military participation examples of which are as follows:

a. Recruiting activities.

b. Publicity tours.

c. Band concerts.

d. Parades.

e. Service social functions.

f. Sporting and charity events.

g. Service social functions such as reunions and dinners.

h. Air Days, Open Days and Ships open to visitors.

i. Lectures by Service personnel.

07449. The event may take place on or off MOD property. All such events are at risk from terrorist attack or interference by extremists.

Application of the Definition

07450. The definition of PME remains deliberately wide to allow HQs and establishments to make a sensible judgement. The vital words are **'the general public'**. There are many minor activities involving elements of the public with the Services that receive no general advance publicity and that can be secured by establishment procedures when they are on MOD property and personal security procedures, such as SHARKWATCH, when off MOD property. Examples are sports fixtures against Service teams within MOD establishments, participation by small numbers of individual Service personnel in local sporting or cultural events or the performance of a small number of musicians (less than 4) at a private function. Such activities are described as Off Site Events (OSE) and are not considered PME. The procedures within this Section need not be applied, advice on OSE security is at Appendix

6. However, if in doubt about the status of an event, advice should be sought from the appropriate PSyA or Command security staffs in sufficient time to allow for **6 weeks** notice of the event to be given to the civil police.

Responsibility for Approval in GB

07451. The notification proforma in the format at Appendix 1 to Annex I and the acknowledgement slip at Appendix 2 to Annex I are to arrive at the civil police force HQ in whose area the event is to take place at least **6 weeks** before the event. The civil police will acknowledge receipt using the proforma at Appendix 2 to Annex I, giving the sponsor the local civil police point of contact for liaison. If the civil police force HQ advises that the military participation in the event should not take place, then the event cannot proceed. In exceptional circumstances where participation in an event is identified with less than 6 weeks notice, it may proceed, only with the unqualified agreement of the civil police force HQ. Examples might include little publicized, short notice sports fixtures or band concerts.

Division of Responsibility

07452. The civil police have overall responsibility for security at PMEs both on and off MOD property. In general, the Service takes the lead in arranging security on MOD property and the civil police take the lead outside MOD property including liaison, when necessary, with the British Transport Police.

Organizers and Event Security Officers

07453. PME sponsors, organizers and participants are to ensure the following measures are taken:

a. Restrict, within the requirements of the event, distribution of information such as forecasts of events e.g. of band concerts, guest lists (particularly important when VIPs will be present), invitations and any other information that might help a terrorist.

b. Ensure that transport (including private cars and minibuses):

(1) Is searched before boarding and loading.

(2) Where possible varies routes to and from entry and exit choke points.

(3) Is ideally parked within a protected MOD establishment or civil police station or is guarded throughout the event by Service personnel positioned outside the vehicles or, in the worst case, located where it can be visited frequently.

c. Provide assistance to the civil police search operations if requested. This may include securing and controlling access to any buildings, rooms, areas and vehicles that Service personnel are likely to use before, during or prior to dispersal

after the event. Personnel may be in uniform or civilian clothes, as agreed by the civil police.

d. Ensure the security of military personnel, equipment and arms at the event and during travel to and from it, using secure overnight storage and accommodation as appropriate.

e. Comply with the Aide Memoire at Annex I.

f. Seek advice on security from their PSyA and Command security staff if required.

Commands

07454. PSyAs and Command security staffs are responsible for monitoring all PMEs to ensure that they are being dealt with correctly. HQ RAF P&SS is responsible for monitoring and co-ordinating security for all PMEs for the RAF.

Civil Police Requests for Large Scale Support

07455. Assistance provided will normally involve those personnel who can be made available without undue penalty. Civil police requests for large scale support must be referred to the relevant HQ who will seek MOD authority if necessary.

Coordination

07456. Outside a Service establishment where more than one Service or unit is participating, the relevant Army HQ in whose area the event is to take place will ensure (in conjunction with the other Services) that responsibility for Service aspects of security are clearly laid down, and co-ordinated, including the appointment of an overall Event Security Officer (ESO) (see Annex I). Whenever possible this will be an officer or WO.

Financial Liability

07457. Where the civil police have a statutory responsibility to provide security, they also have the associated financial liability, regardless of the period of notice involved. For officially sponsored events, civil police would not seek to raise charges. For private engagements run by a commercial sponsor, whether or not for financial gain, the organizer will be responsible for meeting any police charges raised, in addition to the normal charges raised by MOD. If Service attendance at an event is cancelled on civil police advice for security reasons, MOD will assume no financial liability. Commercial sponsors should be advised of the full extent of their liability when booking engagements. It would be improper for any such costs to be met from the Defence budget.

Action to be taken for PMEs outside London District in GB

07458. Completed proforma in the format at Appendices 1 and 2 Annex I are to be sent to the following addressees not less than **6 weeks** before the event:

a. Command security officer. (PME involving RAF).

b. Civil police and own Service local security unit.

c. Relevant Army Division and Brigade HQ.

07459. For the details of points of contact in Army Brigade and Division HQ, supporting Military Intelligence Sections and the civil police force HQ to be informed see the current DCI GEN.

07460. Organizers are to await the civil police force HQ contact officer's notification of the local civil police point of contact and are then to inform the ESO who will:

a. Liaise with the local civil police prior to the event to discuss the proposed security arrangements, in particular any requirement for Service assistance if the event is to take place outside MOD property. If appropriate, a joint reconnaissance of the venue should be conducted by the local civil police commander and the ESO.

b. If the event is not on MOD property, ensure that the military assistance agreed with the civil police is provided.

c. Brief the Service personnel participating in the event on the detailed security arrangements and the duties of personnel provided purely for security prior to the event. The Aide Memoire for ESOs is at Annex I.

d. If an event has to be cancelled for whatever reason then the initial addressees on the notification proforma are to informed as soon as possible.

Action to be taken for PMEs within London District in GB

07461. HQ London District is responsible for informing the civil police about PMEs within the district. Establishments and staffs sponsoring, organising or participating in PMEs within London District are to:

a. Complete the proforma in the format at Appendices 1 and 2 to Annex I and send them to HQ London District and 90 Military Intelligence Section no less than **6 weeks** before the event is due to take place.

b. Appoint an ESO. The Metropolitan Police Division in whose area the event is to be held will contact the ESO prior to the event to discuss security arrangements.

07462. Should the relevant Service Authority wish an event to go ahead, even if the civil police cannot be given 6 weeks notice, negotiations with the civil police about this event are to be conducted through HQ London District. If an event has to be cancelled for any reason, then all addressees are to be informed as soon as possible.

Royal Parks

07463. Service Bands with engagements in the Royal Parks are to travel to London in civilian clothes and change at the locations shown below. Bands should, wherever possible, move in one vehicle. Bands are to change back into civilian clothes before leaving London District. Contact should be made with the relevant location at least **4 weeks** before the event as follows:

a. **St James' Park and Hyde Park.** Wellington Barracks, Birdcage Walk. Camp Commandant: London District Mil ext 3283 or 020 7414 3283.

b. **Regents Park.** Regents Park Barracks, Albany Street. Quartermaster: London District Mil ext 8742 or 020 7414 8742.

c. **Greenwich Park.** Woolwich Barracks, Woolwich (Quartermaster): Woolwich Garrison ext 3296 or 020 8781 3296.

Responsibilities for a PME Overseas

Approval

07464. PMEs overseas, including NI and the ROI, also require similar prior notification so that the civil police or appropriate security organization in the country where the event takes place can be consulted.

Action to be Taken

07465. Establishments and staffs sponsoring, organising or participating in PMEs are to ensure that notification takes place at least **6 weeks** before the event by informing one of the following:

a. The security staff in countries where a UK Command Headquarters is located. (For PME in NI the relevant Bde HQ with an information copy to HQNI).

b. The UK Military Support Unit at a NATO HQ.

c. The British Embassy or High Commission where no UK Command Headquarters exists. (The BRITMILREP Dublin for PME in the ROI).

07466. The PME notification proforma at Appendix 3 to Annex I is to be used. The relevant overseas Command HQ security staff, Military Support Unit, British Embassy or High Commission should then be requested to assume responsibility for:

a. Liaison with the local civil police and relevant security organizations.

b. Granting clearance and approval for the event.

c. Providing a security brief for the sponsor, organizers and participating unit.

07467. The ESO is to take account of relevant paragraphs of the Aide Memoire for ESOs in GB at Annex I when planning participation in a PME overseas.

Security at Open Days

07468. The security of open days poses particular security problems as the very nature of the event gives an extremist the opportunity to enter an establishment under the cover of being a genuine spectator. There is, therefore, a need to plan carefully for such events and involve all the security agencies at an early stage.

07469. The ESO should ensure that the ESyO, Service police, civil police, and local security unit or RAF P&SS are aware of the event. The ESO should also ensure that a security plan is prepared based on the current threat assessment.

NB: The list of police and army units to be notified prior to an event is published in current DCIs and will be updated as required.

Security when Training outside Service Establishments

07470. Training areas are particularly vulnerable to terrorist attack and Alert State measures must be applied rigorously.

Training within GB

07471. Public notification of use of ranges and training areas. Over a long period of time the custom has grown up of publishing, for the benefit (including safety) of members of the public, details of forthcoming training activities on our ranges and training areas. It would clearly be extremely difficult to cease all such notification, particularly in respect of training areas that fall within a national park or where specified routes are open to the public when a range is not in use. However, information published should be kept to the minimum compatible with the above purpose.

Established Training Camps

07472.

a. Due to their fixed and permanent nature, established training camps can be targeted relatively easily by terrorists. In addition, their small or non-existent regular guard or caretaker element can make it comparatively easy for devices to be placed. Where practicable, there should be continuity of occupation, e.g. an advance party of an incoming unit should take over from a rear party of an outgoing unit. It is appreciated that this may be difficult for Reserve or cadet units.

b. In addition to checking the camp thoroughly for IEDs (OP WIDEAWAKE) on arrival or, preferably, by the advance party, the measures relevant to the Alert State in force are to be applied, as appropriate to the size of the party occupying the camp and subject to any specific conditions that may be ordered by the PSyAs and Command security staff of the area in which the camp is located.

c. These measures are to be co-ordinated with the Training Camp Commandant and his Standing Orders as appropriate. When units share a camp, the Commandant may well co-ordinate a joint security plan. These procedures are to be followed if permanent training camps of other Services are used.

d. When the unit or sub-unit leaves the camp for the training area, all doors and window shutters (if applicable) of accommodation vacated should be locked. On return to the camp a check for IEDs should be made (OP WIDEAWAKE), the extent of which would depend on whether or not a rear party had remained in the camp.

07473. Approaches to permanent training camps may be targeted with a view to the placing of booby trap IEDs, RCIEDs or the carrying out of a mortar attack. Particular vigilance should be exercised in relation to the close approaches, in particular route choke points, culverts etc.

Ranges and Training Areas

07474. Due to their permanent nature, range and training areas can be identified relatively easily by terrorists. However, the actual area of the training area to be used would be difficult to identify, albeit that certain fixed facilities provide possibilities for booby traps. When using such areas the following guidance is to be followed:

a. Access points and facilities, e.g. gates, firing points, range consoles, target galleries, huts, kitchens, ablutions and tents etc are to be thoroughly checked on arrival, secured throughout the period in use and checked again on departure if appropriate.

b. Transport is to be guarded or parked in a secure area.

c. On departure the doors and window shutters (if applicable) are to be locked and the keys returned to the relevant authority.

Private Land

07475. Training on private land is generally unpredictable and would be difficult for a terrorist organization to target, but the relevant Alert State measures should be enforced throughout the training period.

Adventurous Training

07476. Unless there are good reasons for not doing, personnel on adventurous training should adopt the principle of anonymity. The expedition should, therefore, be civilianized in every respect (including clothing and vehicles). Rules for adventurous training and expeditions are contained in DCIs reissued annually. The expedition leader will need to read the relevant DCI in the early planning stages of an expedition; copies of the DCI should be held by establishment training staff. Whenever possible unattended vehicles should be left in a secure area. However, in all cases vehicles are to be thoroughly searched if they have been left unattended.

Major Sports Events

07477. Sponsors of major sports events where the public have or could gain access, are to treat the event as a public military event (PME) and take action accordingly.

Training outside GB

07478.

a. **Training in Germany (excluding adventurous training).** Before deployment, units are to be informed of the KEENWIND state (the BFG Alert State system similar to BIKINI) by PSyAs and Command security staff.

b. **Overseas training exercises other than in Germany (excluding adventurous training).** Overseas training exercises outside Germany fall into two categories: those taking place in countries where a UK command or training structure exists, e.g. Cyprus or Kenya; and those where no such structure exists, e.g. France and Norway.

c. **Countries with a UK Command or training structure.** Exercise recce teams will be briefed on the threats to security and the appropriate protective counter measures by the receiving Command or training unit. Relevant security aspects are to be considered in exercise planning and included in instructions and briefing. Any planning problems should be referred to the Command security staff. If appropriate, the receiving Command or training unit is to supplement this with a more detailed briefing on the unit's arrival in country.

d. **Countries without a UK Command or training structure.** As in sub-paragraph 07478c above but the action is to lie with the sending Command and the training unit.

e. **Overseas adventurous training expeditions.** The relevant adventurous training staffs will pass details of such projects to the relevant security staff, who will obtain threat assessments, as necessary, and pass them on together with security advice for inclusion in their briefing of the expedition leader.

f. **Overseas sports events.** Organizers or sponsors of military teams participating in sports events overseas are to seek security advice from the relevant security staff. This advice should be sought as early as possible in the planning stage.

Counter Terrorist Search

Introduction

07479. Counter terrorist search (CTS) has been a significant component of security force operations in NI since 1970. After the bombing of the Grand Hotel in Brighton in 1984 and terrorist attacks on military installations in Great Britain and elsewhere, CTS measures have become an important part of military counter terrorist operations wherever a threat of

terrorist attack exists. Military CTS capabilities have been developed primarily to defeat the Irish republican terrorist threat, but are equally capable of countering threats from other terrorist groups.

Terminology

CTS

07480. Military CTS involves the use of systematic procedures to find terrorists and their resources and to confirm the presence or absence of bombs within specified boundaries. The objectives of CTS include obtaining evidence, depriving terrorists of their resources, providing information or assuring a facility is safe to use. It is conducted by trained personnel who may be supported by other agencies including intelligence, Arms and Explosive Search Dog Teams, EOD Teams, Electronic Counter Measures and Aerial Photographic Reconnaissance. The following terms are commonly used:

a. **High Risk Search (HRS).** HRS operations are searches carried out when it is assessed that there is a high probability of a bomb, booby trap or improvised explosive device (IED) being present.

b. **Low Risk Search (LRS).** LRS operations are searches carried out when it is assessed that there is a low probability of a bomb, booby trap or IED being present.

c. **CTS Awareness (CTSA).** CTSA is an individual's knowledge and use of basic search measures to deter, detect and defeat a terrorist attack.

d. **Defensive CTS.** Operations carried out to protect potential targets, including personnel and property, are defensive CTS. Such operations include both random search measures to deter the terrorist, and any search instigated to ensure that a specific area, route or venue is clear of terrorist devices.

e. **Offensive CTS.** Offensive CTS operations are investigative operations mounted to achieve any of the following:

(1) Deprive terrorists of their resources.

(2) Gain evidence that may be used in a prosecution.

(3) Obtain information for intelligence purposes.

f. **Search co-ordinators.** The role of the search co-ordinator is to integrate search operations into the commander's overall plan and to provide liaison between agencies at the appropriate level. The degree of knowledge will depend on the position held. Training is provided for appropriate appointees on Command HQ and formation staffs, operations officers of specified units deploying on operational tours such as in NI, and Royal Engineer and Service police officers in appointments within units involved in operational search.

g. **Search Advisors.** Search Advisors are trained to provide detailed CTS advice on the operational deployment and employment of search teams for which they are responsible. Search Advisors must be involved in the planning of search operations, they will direct and issue orders to search teams involved, and should provide the link between search teams and the all arms commander on the ground throughout the operation.

Policy

Civil Police

07481. In the UK, Chief Constables are responsible for CTS operations within their own areas. The Home Office provides guidance to police forces on CTS matters and on the procedures to be used by police forces requiring military CTS assistance.

MOD

07482. Within MOD the Army Department takes the lead on CTS issues. Specific responsibilities are as follows:

a. **Joint Service Policy and Resources Committee (JSSPRC).** JSSPRC considers and endorses Joint Service CTS policy and resource requirements. Implementation of Joint Service policy, and provision of suitable resources to implement endorsed policy once agreed, is a Single Service responsibility. JSSPRC reports through the Joint Service Explosive Ordnance Disposal Policy Committee (JSEODPC) to DCDS(C). The Chairman of JSSPRC is nominated by the Engineer in Chief (Army) (EinC(A)).

b. **Director Military Operations (DMO).** DMO (MO2) sets the tri-service CTS policy and is the MOD focus for co-ordination of CTS operations. DMO provides the link between MOD and other government departments and controls Military Aid to the Civil Power (MACP) support under arrangements designated in the MACP Handbook. DMO is responsible to Assistant Chief of the General Staff (ACGS) for ensuring the implementation of Joint Service policy within the Army Department.

c. **Director of Naval Security and Integrated Contingency Planning (DNSyICP).** DNSyICP is responsible to the 2SL/CINCNAVHOME for implementation of Joint Service CTS policy within the RN.

d. **Engineer in Chief (EinC(A)).** EinC(A), through DMO, will normally provide military CTS advice to all government departments and provides the Chairman and Secretariat for JSSPRC. EinC(A) sponsors all CTS training, which is carried out under the direction of the Commandant Royal School of Military Engineering (RSME) at the National Search Centre (NSC) Chattenden. NSC is the national focus for provision of CTS advice.

e. **DCDS (EC).** DEC(SP) sponsors all CTS equipment programmes.

f. **Defence Procurement Agency (DPA). DPA** is responsible for the procurement of all CTS equipment.

g. **Air Officer Security and Provost Marshall (RAF) (AOSy&PM(RAF)).** AOSy&PM(RAF) is responsible to Assistant Chief of the Air Staff (ACAS) for implementation of Joint Service CTS policy within the RAF.

Theatres and Commands

07483. Theatres and Commands are responsible for CTS policy and operations within their commands. Commanders are to ensure that:

a. An officer within his HQ, where necessary also within subordinate formation HQ, is nominated and trained as a Formation Search Co-ordinator (FSC). This officer should be the focus for co-ordination of advice on search policy and of CTS operations.

b. Adequate CTS resources are established in theatre to counter the assessed threat. This includes provision of manpower and equipment.

c. Procedures exist for the conduct of CTS operations.

d. CTS and CTSA direction and advice is provided to units.

Units

07484. Unit commanders are to ensure that all personnel are trained to be CTS aware, and are responsible for security arrangements and procedures within the unit. A Unit Search Co-ordinator (USC), normally the Unit Security Officer, is to be appointed to be responsible for CTS arrangements and for CTSA training within the unit. Units should seek CTS and CTSA advice and assistance where necessary from their FSC.

CTS Resources

07485. There is a wide variety of resources that can contribute to CTS operations. These resources are not available in all theatres, but are tailored to meet theatre requirements. The types of resource and their capabilities are outlined in this section.

Police

07486.

a. **Civil Police.** Civil police in GB and NI have the capability to carry out LRS using Police Search Teams (PSTs) under the control of a Police Search Advisor (POLSA). Their capabilities are similar to those of Service Police Search Teams (SPSTs). The capabilities of civil police in other theatres will vary.

b. **Service Police.** Service Police have the capability to form SPSTs. Such teams are trained and equipped to carry out LRS. Their employment is primarily

for defensive search operations for specific events. SPSTs should operate under direct command of a trained Service Police Search Advisor (SPSA) or Royal Engineer Search Advisor (RESA). SPSTs are deployed by the Army and the RAF.

c. **MOD Police (MDP).** MDP have POLSAs and low risk PSTs deployed at certain locations in UK. Additional teams can be tasked centrally by Territorial Operations Branch for MDP HQ.

All Arms

07487. All units have some search capability. This capability should include at least CTSA trained personnel. The all arms capabilities are:

a. **CTSA.** Personnel trained to be CTSA can carry out basic CTS procedures using simple equipment (e.g. torches and mirrors) provided under local arrangements. These should only be employed in random low risk searches in areas with which they are familiar. These personnel cannot be formed into search teams and are not a substitute for a qualified, fully equipped, search team.

b. **Patrol Search.** Patrol Search is an all arms LRS capability currently only employed in NI but which could be employed in other theatres if the threat warranted it. It involves search by all arms units as part of normal patrol activity, using limited types of search equipment. The patrol search capability is limited to route checks, rummage search of areas, and vehicle and personnel searches, under direction of their unit commanders. Training for patrol search is carried out within units under direction of RSME. Patrol Search operations should be co-ordinated by the Unit Search Co-ordinator (USC).

c. **All Arms Search Teams (AASTs).** An AAST normally consist of eight personnel trained and equipped to carry out designated LRS operations. The training and capabilities of AASTs is tailored to meet the requirements of the Teams' different will vary by operational areas. AASTs operate under the direct control of a qualified Unit Search Adviser (USA) or a RESA, and are currently deployed in NI and Cyprus.

Royal Engineers (RE)

07488. RE provide a comprehensive capability for CTS operations. RE are primarily responsible for HRS and searches of a specialist nature but also provide support and advice to all arms search operations where necessary. The RE capability consists of:

a. **RE Search Teams (RESTs).** A REST consists of six personnel trained and equipped to carry out HRS and LRS operations within their designated theatre. RESTs operate under the direct control of an RE Search Advisor (RESA). Their deployment should be controlled by an RE Search Co-ordinator (RESC). RESTs are currently, available in GB, NI and Cyprus, but GB based assets can be deployed elsewhere if necessary.

b. **RE Specialist Search Equipment Teams (RESSETs).** RESSETs are RE personnel equipped with specialist equipment. They can be deployed, normally in pairs, to assist in HRS or LRS operations. RESSET operators are trained members of a REST and their deployment should be controlled by a RESA. Formed RESSETs are currently only available in NI, however in GB 33 Engr Regt (EOD) have access to a similar range of equipment.

Supporting Agencies

07489. A wide variety of agencies may be involved in search operations. Search advisors will suggest which supporting assets might be necessary. The following, which is not a comprehensive list, provides some examples:

a. **Dogs.** CTS operations may be supported by dogs trained in the detection of weapons, ammunition and explosives. The Army, RAF Police, MDP and UK civil police all have dogs for this task.

b. **EOD Team.** Where EOD action may be required the involvement of the appropriate JSEOD team or Ammunition Technical Officer (ATO) should be considered.

c. **Specialist Electronic Counter Measures (ECM).** Where necessary, and where a threat exists, specialist ECM assets supported by an IEDD team, should be deployed to support a CTS operation.

d. **Reconnaissance Intelligence Centre (RIC).** In certain circumstances RIC assistance may be appropriate prior to a CTS operation.

Requests for Assistance

Assistance to Military Establishments and Units

07490. Requests for CTS assistance should follow the chain of command. Advice should be sought from FSCs who should normally assist in carrying out a risk assessment in conjunction with the civilian police Special Branch, PSyA and Command security staffs and the establishment or unit concerned. The level of risk is determined by considering:

a. **Threat Level.** The threat level is generally assessed by considering terrorist intentions and capabilities. Special Branch or PSyA and Command security staffs will consider the level of threat generally, and the attractiveness of the target (a person or an event) to terrorist groups.

b. **Vulnerability.** The following factors contribute to vulnerability:

(1) **Predictability.** Both periodically occurring events and those that are widely publicized are vulnerable, particularly if the people attending are attractive targets. Events occurring at less than five days notice, or with little public knowledge or prior indication are less vulnerable.

(2) **Security.** A lack of security or freedom of access will provide opportunities for terrorists to exploit potential targets.

07491. If the risk warrants it, a fully trained search advisor should be employed to determine the type of search required.

Assistance to Police

07492. In the UK, military CTS assistance to police or other civil organizations is carried out under MACP arrangements as follows:

a. **NI.** GOC NI can employ the Army to carry out CTS under MACP as a standing arrangement.

b. **GB.** The method of providing CTS assistance depends upon the degree of urgency:

(1) **Planned Operations.** Requests from the civil police are directed to DMO (MO2), who will then task as appropriate.

(2) **Immediate Operations.** When terrorist activity is identified, a request for immediate RE assistance may be made through DMO or direct to the Joint Service EOD Operations Centre (JSEODOC) at Didcot (civil telephone 01235 819191 extension 3360/1/2 or Didcot Military 3360/1/2) which is manned on a 24 hour basis. JSEODOC has the authority from DMO to task CTS assets from 33 Engineer Regiment (EOD) for an immediate task.

This page intentionally blank

ANNEX A TO SECTION IV TO CHAPTER 7

CONTINGENCY PLANNING FOR UNEXPECTED EVENTS

Scope of Planning

1. Establishment contingency plans must lay down procedures for:

a. Evaluating the threat on receipt of a bomb or attack warning. Every warning must be investigated unless or until it is proved to be a hoax or otherwise.

b. Deciding how to respond to threats.

c. Implementing the response.

d. Informing all concerned if evacuation is necessary.

e. Directing personnel away from the threatened areas to safe zones.

f. Ensuring the speedy arrival of emergency services, e.g. civil police, Ammunition Technical Officer (ATO), fire or ambulance as required.

g. Appointing an Incident Control Officer (ICO), (in working hours the unit security officer (USO)), to be responsible for directing the response to the threats. More than one control officer may be necessary in large depots or establishments.

h. Establishing a control centre with adequate internal and external communications.

Evacuation

2. Arrangements for evacuation should be pre-planned and practised. There are two options:

a. **Partial evacuation.** This response may be appropriate when the location of the bomb or the likely target to be attacked, is known or suspected. Safe assembly areas should be identified in advance.

b. **Total evacuation.** Contingency plans should allow for the direction of personnel away from the danger zone.

3. Safe assembly areas of evacuation should be searched and cleared before moving personnel to them and where possible the approach routes should also be cleared. Care

should be taken to avoid vulnerable areas such as car parks, refuse bins, etc (that could have explosives planted in them) when moving personnel during evacuation procedures.

Liaison and Notification Drills

4. Planning should take account of the need for liaison with local police, fire and ambulance services. If the decision is taken to evacuate, the control centre should notify the police and ATO, and alert the fire services.

Service Precautions During Partial or Total Evacuation

5. Unit arrangements must ensure that if evacuation of a security area or building is necessary, all protectively marked material is secured in the appropriate containers before evacuation. If an explosion or fire makes this impossible, doors and windows must be securely fastened.

Stand-down

6. 'Stand-down' and 'lock up' drills should be organized in advance, either to order the return to duty, or to disperse, with further instructions as to when to return.

Detailed Guidance

7. Guidance on the detailed action to be taken on the discovery of an explosive device is given at Appendix 1 to Annex H.

ANNEX B TO SECTION IV TO CHAPTER 7

SPECIAL PRECAUTIONS FOR PROTECTION OUTSIDE MOD ESTABLISHMENTS

General

1. The greatest protection will stem from maintaining individual vigilance and avoiding predictable patterns of activity. Common-sense and alertness are of paramount importance. Where regular patterns of activity are unavoidable Service personnel should adopt positive protective measures, e.g. by forming organized groups with nominated 'look-outs' at times of high risk. In such circumstances it may be necessary for units to consult the civil police.

2. Guidance on protection outside MOD establishments is given below. The detailed application of this guidance will depend on local circumstances.

Unit Movement

3. Units should:

a. Avoid regular patterns of timings and routes.

b. Avoid regular predictable parking arrangements.

c. Ensure they do not present an easy target by adopting other predictable patterns of activity, for example, by failing to guard empty vehicles or post sentries when groups of personnel are vulnerable.

d. Ensure that personnel stay alert.

e. Adopt a system for reporting any suspicious activity and for taking action on such information.

f. When using hired transport.

(1) Search vehicles before use.

(2) Check the identity of drivers with employers.

(3) Check the arrangements for the carriage of baggage and equipment.

g. Consider the need to take special precautions to avoid being surprised when using public transport. These might include, for example, making arrangements for

the searching of railway stations and carriages before use, avoiding advance publicity, etc.

h. Obtain advice from the civil police, Service police or local security unit as necessary.

Drivers

4. The following guidance for drivers may be applied by units to personnel whether on duty in Service vehicles or in private cars. Drivers should:

a. Avoid leaving a vehicle unattended outside a protected area. When this is impossible, carry out a search before using the vehicle.

b. Never leave a lockable vehicle unlocked.

c. Look out for areas along routes that could be used for an ambush.

d. Observe other vehicles and people and look out for suspicious activities. Avoid and then report any suspicious activity.

e. Carry a mobile phone or know the location of public call boxes along routes and carry relevant telephone reporting numbers and suitable coins/cards.

f. Avoid displaying military connections when using private vehicles. For example, do not display Service badges or stickers or leave items of uniform or equipment where they can be easily seen.

5. Additional points for staff car drivers are at Appendix 1.

Training

6. Training often involves the regular use of ranges and training areas. The nature of range work tends to compel units to follow predictable patterns of activity because regular use of butts, firing points, etc, is unavoidable. When planning training, units should consider the following:

a. Searches and checks of ranges and training areas before use.

b. The requirement to guard areas after searches and checks.

c. The requirement for sentries where groups of Service personnel may be vulnerable, e.g. in bivouac areas.

d. Additional vehicle guards.

e. Liaison with emergency services when training is planned in more remote areas.

Sporting Activities

7. Sporting activities, like training, may produce predictable patterns of activity. Units should consider:

a. Staggering sports periods to avoid, for example, regular Wednesday afternoon activities.

b. Searching sports areas and arenas, etc, before use and, in particular, changing accommodation that may need protection while in use.

c. Paying particular attention to routes frequently used for running, orienteering, etc.

d. Assessing the risk involved in the regular participation of individual personnel in civilian teams and events.

Social Activities (Organized and Private)

8. All social activity involves risk and units should consider the security implications, in particular the following:

a. The requirement to brief all concerned on the risks involved when using public houses, clubs, etc. At times it may be necessary to lay down that Service personnel go out in groups and that each group has an agreed lookout responsible for the security of the group, sometimes known as SHARKWATCH.

b. The need to organize social functions with care, particularly official ones and to draw up a proper security plan in conjunction with others, as necessary, again it may be necessary to adopt SHARKWATCH.

c. The need for liaison with the civil police and, where appropriate, with the managers of frequently used local places of entertainment, who may agree to participate in SHARKWATCH.

Travel on Duty, Leave and Recreation

9. Travel outside the unit frequently involves individuals or loose groupings of individuals forming at railway and bus stations, etc, on weekends and at stand-down periods. While there can be no substitute for individual vigilance, units should give briefings to personnel on points to remember, including:

a. The need to avoid displaying military connections. Examples include:

(1) Wearing uniform or items of uniform unnecessarily in public.

(2) Using Service issued suitcases, rucsacs or kit-bags when this is avoidable.

(3) Careless talk.

b. The need to exercise particular care when using public transport. Control of baggage should be emphasized.

c. The need for individuals to take the same security precautions with their private cars as with Service vehicles (see paragraphs 3 and 4).

ANNEX C TO SECTION IV TO CHAPTER 7

ADVICE ON HANDLING ANONYMOUS TELEPHONE CALLS WITH WARNINGS OR THREATS

1. **General.** Suspicion that an IED may have been planted within an establishment often results from an anonymous telephone call or bomb warning. Any such call must be taken seriously even though subsequent investigation may reveal a false alarm or hoax. Terrorists have used hoax calls in the past to test reactions, observe evacuation procedures and encourage complacency. The following definitions are in general use:

a. **Bomb warning.** This term refers to the manner in which the incident starts. The majority of bomb warnings are received by telephone but the term also covers the alarm that is raised on the discovery of a suspect item.

b. **Bomb scare.** After a bomb warning has been investigated and discredited, any precautionary measures may be relaxed and normal activity resumed. This incident would be termed a "bomb scare."

c. **False alarm.** A suspect item is discovered and an EOD operator tasked. If, after investigation, the item turns out to be completely innocent, i.e. left without evil intent, it is declared as a "false alarm".

d. **Hoax.** A hoax is an item constructed to resemble an IED but containing no explosive or dangerous substance.

2. **Action on receipt of a call.** On receiving an anonymous call you should:

a. Try to keep a verbatim record of the conversation.

b. Attempt to obtain the name of the caller and their address and telephone number or a contact point. You should point out to the caller that by giving these details they are indicating that it is a genuine warning.

c. Attempt to keep the caller talking on the line and elicit further information if possible.

d. Keep the line open after the caller ends the call; this will make it easier to trace the call.

e. Summon assistance to trace the call (through a telephone exchange) and to corroborate the facts and your opinions.

f. Comply with any request by the caller to be connected with another extension but if possible monitor the call and alert the Service Police, MDP, civil police or ESyO.

g. **Warning containing a codeword.** If the warning contains a codeword, the codeword used by the caller should be verified immediately with the civil police.

2. **Facts to be obtained.** During the course of the call the recipient should attempt to establish the following:

a. Establishment involved.

b. The exact location of the device.

c. The time it is due to detonate.

d. What sort of device it is.

e. The specific reason for the attack.

f. Identity of the caller.

g. Why the caller is giving a warning.

3. **Other useful facts.** Security staffs will require details of the following:

a. **Voice characteristics.**

(1) Was the tone normal or not?

(2) Did it sound disguised or muffled?

(3) Was it high pitched or stuttering or otherwise indicative of nervous tension?

(4) Was it slurred or indicative that the person was under the influence of drink or drugs?

(5) Was there evidence of excitement in the informant's voice?

(6) Did the caller give the impression that the message was being read out?

(7) Did the voice have a pronounced or recognisable accent?

(8) Was the caller male or female?

(9) Was the caller young or old?

b. **Background noises.**

(1) Was there any sound that would indicate someone else was with the caller, e.g. prompting or giggling in the background?

(2) Was there any background noise of road traffic, aircraft, radio or juke box etc?

c. **Caller's knowledge of circumstances.** Did the caller display a detailed knowledge:

(1) Of the establishment, particularly its role and layout or personalities.

(2) The device.

d. **Recording information.** After providing the security staff or police with details of the call the operator or recipient should immediately make a full written record of the conversation and the impression gained of the various characteristics outlined above.

4. **Threat call checklist.** A suggested threat call checklist is at Appendix 1. A supply of these forms should be readily available, especially at locations where threat calls are likely to occur, e.g. telephone exchanges and guardrooms.

5. **Immediate response drills** After receipt of an anonymous call or bomb warning the following action should be taken:

a. Inform the civil police immediately using the 999 system. (The civil police will inform the JSEODOC who will place an EOD team on standby).

b. Inform the appropriate HQ, local security unit and Focal Point depending on local SOPs.

c. Evacuate all or part of the establishment under threat by implementing an evacuation plan.

d. Carry out establishment level search to confirm that an IED has been placed. Guidance on counter terrorist search awareness is included in Annex J.

6. **Use of BT '1471' facility.** When a call is received on a direct dial BT line the recipient should dial 1471 immediately after the call, in order to trace the call (assuming the caller has not barred this facility).

This page intentionally left blank

APPENDIX 1 TO ANNEX C TO SECTION IV TO CHAPTER 7

CHECKLIST FOR TELEPHONED BOMB WARNINGS

OBTAIN AS MANY OF THE FACTS LISTED BELOW AS POSSIBLE

(Switch on Tape Recorder if Connected)

1. EXACT WORDING OF THE THREAT: .....
.....
.....
.....
.....
.....

(KEEP THE TELEPHONE LINE OPEN - even if the caller disengages).

2. **QUESTIONS TO ASK:**
   a. Where is the bomb right now? .....
   b. When will it explode? .....
   c. What does it look like? .....
   d. What kind of bomb is it? .....
   e. What will cause it to explode? .....
   f. Did you place the bomb? .....
   g. Why? .....
   h. What is your name? .....
   i. What is your address? .....
   j. What is your telephone number? .....

3. Where *automatic number reveal* equipment is available, record the number shown:

   .....

4. **INFORM YOUR SECURITY CONTROL (IAW Establishment Orders) - Record the Name and Telephone Extension of Person Informed**

Name:		**Ext.**	

5. **INFORM CIVPOL BY 999 CALL (if required by Establishment Orders):**

Time Informed:	

This part of the form should be completed once the caller has hung up and the Establishment Security Control/CIVPOL have been informed.

6. **DATE AND TIME OF CALL:**	Date and Time:	
Length of call:	Length:	
Extension on which call received:	Ext:	

ABOUT THE CALLER

Sex of caller? Male ☐ Female ☐

Nationality? ..... Age? .....

THREAT LANGUAGE

Well Spoken ☐ Irrational ☐ Taped ☐

Foul ☐ Incoherent ☐ Message Read by Threat Maker ☐

CALLERS VOICE

Calm ☐ Crying ☐ Clearing Throat ☐ Angry ☐

Nasal ☐ Slurred ☐ Disguised ☐ Stutter ☐

Excited ☐ Slow ☐ Laughter ☐ Lisp ☐

Rapid ☐ Deep ☐ Familiar (see below) ☐ Hoarse ☐

Accent ☐ What Accent? .....

If the voice sounded familiar, who did it sound like?

BACKGROUND SOUNDS

Street Noises ☐ House Noises ☐ Animal Noises ☐ Clear ☐

Motor ☐ Voices ☐ Static ☐ PA System ☐

Factory Machinery		Office Machinery		Booth		Music	

Other (Specify) .....

REMARKS

.....
.....
.....
.....
.....
.....

Signature: ..... Date: .....

Name in Block Capitals

This page intentionally left blank

ANNEX D TO SECTION IV TO CHAPTER 7

ACTION UPON DISCOVERY OF A SUSPECT POSTAL BOMB

General

1. In basic terms, a postal bomb is an IED that has been delivered to an individual or organization though the mail system. It is likely to have been handled by several people during transmission and will be constructed to withstand such man-handling.

2. Being an anti-personnel device designed to detonate on opening, the person discovering a postal bomb is likely to be quite safe provided that no attempt is made to open or tamper with the object. Once declared as suspect, the general procedures for dealing with an IED should be observed.

Immediate Response Drills

3. Having decided that an item of mail is suspect, the following actions should be taken:

   a. Place the object on the nearest level surface, such as a table or the floor.

   b. Without further handling the object, make a detailed note of any markings and characteristics, including size, post mark etc.

   c. Evacuate the area, leaving all doors and windows open.

   d. Carry out the IED immediate response drills.

4. **Do not**:

   a. Attempt to open the package.

   b. Attempt to carry the object out of the building.

   c. Attempt to place the object in a bucket of water.

   d. Attempt to cover the object with sand, or sandbag around the object, or surround the object by steel cabinets or other furniture, as this is likely to enhance any explosive shrapnel effect.

5. If suspicions are aroused once the package has been partially opened, or the contents partially removed, carry out the same immediate reaction drills.

6. Advice on postal bomb recognition is at Appendix 1.

APPENDIX 1 TO ANNEX D TO SECTION IV TO CHAPTER 7

POSTAL BOMB RECOGNITION

Types of Postal Bomb

1. A postal bomb is essentially an anti-personnel weapon that is usually designed to explode at the moment of opening. The device will invariably contain an explosive charge, a detonator or igniter to initiate the charge and some form of triggering mechanism. The triggering mechanism will probably employ an electrical igniter system, a percussion device involving the release of a spring-loaded striker, or a simple frictional method of ignition.

Superficial Appearance and Other Indications

2. The sender of a postal bomb will take great care to make its appearance as innocuous as possible. The envelope may be professionally embossed suggesting that it comes from a bonafide source, and the recipient's address may also be printed or typed. As the first identification of a postal bomb is likely to depend totally on the recipient becoming suspicious when the mail is first examined, personnel should be alert to the following aspects that could indicate receipt of a letter bomb:

a. If the point of origin gives cause for doubt.

b. If the manuscript of the sender is unusual.

c. If the balance of the package is uneven.

d. If the package seems very heavy for its size.

e. If there is any springiness in the top, bottom or sides of the package or letter (but do not bend excessively).

f. If wires protrude from it.

g. If there is a hole (like a pinhole) in the package wrapping or envelope.

h. If there are grease marks on the envelope or parcel wrapping (from the "sweating" of the explosive).

i. If it smells of almonds or marzipan.

j. If the package is thought to contain a book that is not expected.

k. If the flap of an envelope is stuck down completely (usually there is an ungummed gap at each end of the gummed flap).

3. Additionally look for the following when examining letters.

a. The feel will indicate whether there is only folded paper inside the envelope (that will show that it is all right). A bomb will probably have stiffening, e.g. by cards or the feel of metal.

b. Letters usually weigh up to 28 grams. Postal bombs will usually weigh more than 56 grams and therefore need more than the usual postage stamps. They will tend to be unusually thick (e.g. 3.2mm or more) and are likely also to feel lop-sided.

c. If an envelope contains an inner envelope addressed to an individual, this should be examined again for the signs listed. An inner envelope that is tightly taped or tied with string is also typical of a bomb.

4. It may not be possible to feel any solid objects in the package since these are not essential ingredients and, if present, may be shielded by padding. It is also important to realize that the envelope and its contents may be quite flexible.

Operation of the Device

5. A postal bomb is usually designed so that the action of opening it causes an immediate explosion. The actions relied upon to operate the device may be summarized as follows:

a. **Tearing apart the envelope.** This action can either operate a simple electrical switch or release the spring-loaded retainer of a striking mechanism.

b. **Pulling out a tucked in envelope flap.** The interior part of the flap may be connected by a thread to an electrical switch, to a friction device or to the retainer of a percussion striker. It should be noted that, in some devices, the necessary pull on an operating thread is very small indeed.

c. **Using a paper knife.** The use of a paper knife could pull a thread, as in sub-paragraph 4b above.

d. **Removing the contents of an already opened envelope.** This action could achieve the same results as those referred to in sub-paragraphs 4a and 4b above. In this context, any unusual resistance to the removal of the contents could be significant.

Potential of a Postal Bomb to Kill

6. Postal bombs may be designed either to kill or to wound and frighten. Lethal letter bombs invariably contain powerful explosive; those not designed to kill may contain either a small charge of high explosive or even a detonator alone, or a quantity of incendiary or flash material. The characteristics of both types of bomb are as follows:

a. **Lethal postal bomb.** The designer of a postal bomb normally strives to avoid suspicion by keeping the package as thin as possible and using standard envelope sizes. But technical considerations and the need to include an adequate explosive charge mean that a lethal bomb less than about 3.2 mm thick is unlikely to be used. Lethal bombs are likely to weigh 43-84 grams (they can, of course, be heavier) and would cause the recipient injury, severe shock and possible death. One that was 84 grams or more would almost certainly kill. While these weights, which are based on past experience of these devices, are still most likely to be encountered, modern developments in explosives and electrical circuits does mean that smaller devices could also be lethal.

b. **Postal bombs designed to wound, shock or frighten.** Bombs not designed to kill are made in the same way as lethal ones but may be of the same flexibility and thickness (about 1.6mm) as an ordinary letter. Those that contain a high explosive could be expected to cause injury to hands and possibly to the eyes. Others containing incendiary or flash material could produce a brilliant flash followed by fire but not a dangerous blast, injury being limited to burns on the hands and possible harm to the eyes.

This page intentionally left blank

ANNEX E TO SECTION IV TO CHAPTER 7

SAMPLE GUIDE TO IDENTIFICATION OF IMPROVISED EXPLOSIVE DEVICES (IED)

***DO NOT** MOVE OR TOUCH ANY SUSPECT OBJECT THAT HAS NOT COME THROUGH THE POST. IT MAY BE BOOBY-TRAPPED.*

Suspected IED Received in the Mail

1. A postal package or letter should be treated as a suspect in the following circumstances:

a. Point of origin; e.g. the post mark or name of sender, being particularly careful with items postmarked from Northern Ireland that are 2 cm or more in thickness. If from an unusual point of origin or sender, treat as suspect, but do not return to the sender for validation.

b. Handwriting of sender; if this indicates a foreign style of writing and as such is not usually received.

c. Balance; if the package or letter is lop-sided.

d. Weight; if there seems to be excessive weight for size.

e. Protruding wires (even well prepared devices can get damaged in transit).

f. If there is a small hole (like a pinhole) in the package wrapping or enveloping.

g. If there are grease marks on the envelope or parcel wrapping (from the "sweating" of explosives).

h. If there is a smell of almonds or marzipan.

i. If the package is suspected of containing a book.

j. If the flap of the envelope is stuck down completely (usually there is an ungummed gap of about 3mm).

k. To cater for modern explosives, a packet may be less than 2cm thick, otherwise the above characteristics may be similar.

l. In addition, in the case of letter, the feel of the letter will indicate whether there is only folded paper inside the envelope (that will show that it is alright) or if there is some stiffening material or metal.

m. Letters usually weigh up to about 30gms. Effective postal bombs will weigh about 60gms or more.

n. If on opening an envelope, there is an additional envelope addressed personally to someone, this should be felt again for signs of the pointers indicated above. An inner envelope that is tightly taped or tied with string should be treated as suspect.

2. If suspicions remain, place the package on the nearest horizontal firm surface. Leave the room, having opened the windows if possible. Leave the door open but prevent other people entering. Call the Security Officer or a member of the Guard Force.

a. **Do not** take the package to the security officer or to the guardroom.

b. **Do not** put the package in a bucket of water or sand.

c. **Do not** bend or flex the package.

d. **Do not** operate electrical emission equipment such as radios or mobile phones within 25 metres of the suspect device.

3. If you have started to open the package when suspicions are aroused, put it down gently on a firm surface, protecting the face and body if possible by reaching around a desk or steel cupboard or by leaving the room and reaching around the door post into the room. Leave the room, leaving the door open. Prevent others entering. Call the Security Officer or a member of the Guard Force. If it is prudent to lock the room, give the key to the Guard Force or Security Officer.

IED other than Postal Devices

4. An IED may be of any size and may exhibit any or none of the following characteristics:

a. **Visible characteristics.** IEDs are often assembled with adhesive tape. The following may also be present:

(1) Wiring, switches, torch bulbs, electronic circuits.

(2) One or more dry cell batteries.

(3) Container of liquid.

(4) Clock or clockwork timer.

(5) Plastic-covered cord, similar to washing line or domestic electric cable.

(6) Cylindrical tubes, cardboard or paper-wrapped.

(7) Small plywood box (approximately 15 x 10 x 4cms).

b. **Sound.** Noises may be produced by the device prior to it exploding or igniting.

c. **Smell.** Some explosives have a characteristic smell similar to almonds or marzipan. The smell of petrol may be present. Any pungent smell is suspect. However, some modern explosives have no smell.

This page intentionally left blank

ANNEX F TO SECTION IV TO CHAPTER 7

MINIMUM SECURITY STANDARDS AT ARMED FORCES CAREERS OFFICES

1. **Front door.** The front door is to have:

   a. A minimum of a 5-lever deadlock fitted.

   b. Laminated glass fitted or glass covered with anti shatter film (ASF) and/or bomb blast net curtains (BBNC).

   c. Remote control locks fitted where entrance is away from main entrance or cannot be seen from main reception.

   d. A CCTV camera with appropriate lighting fitted to cover the entrance with a monitor located in the reception area, whenever the entrance is away from the main door or cannot be seen from main reception.

2. **Entrance halls and passage ways.** All internal entrance halls and passages should have good lighting to assist staff when checking for IEDs. Similarly, immediately adjacent external passage ways or entrance halls, where devices could be concealed, should be illuminated and capable of being viewed from within by use of mirrors or windows and, if considered necessary by a specialist survey team, monitored by a CCTV system.

3. **Glass frontages and windows.** There is no standard security template for the protection of window displays. Careers offices vary in size and location and each display window must be assessed separately. Specialist survey personnel will assess individual requirements. Those windows and fanlights not used for display purposes are to be protected by ASF, bomb blast curtains and bars, as necessary.

4. **Rear doors.** Rear doors are to be fire resistant and of solid construction. Heavy duty bolts and 5-lever deadlock are to be fitted unless the door is designated as a Fire Exit, when a Fire Safety or Fraser Bar is to be fitted. Any window or aperture in the door is to be covered by a metal grille. Finally, if the door is in regular use a heavy duty digital lock is to be fitted.

5. **Letter boxes.** All letterboxes are to be sealed and arrangements made for the mail to be collected from the local Post Office or delivered by hand during office working hours.

6. **External office ventilation.** All external office ventilation intakes/exhausts are to be protected by metal grilles.

7. **Reception desk panic button.** The reception desk is to have a concealed panic button fitted that sounds a muted alarm to summon assistance from other members of staff.

8. **Garages and parking.** Ideally, all careers office vehicles should be garaged in a secure parking area e.g. at a police station, or in unmarked lockable garages. The garages should, if practicable, be monitored by a CCTV camera system and/or an audible alarm. Where neither secure parking or lockable facilities are available then vehicles should be parked in discrete parking areas up to 15 minutes away from the careers office. Whenever possible the "buddy" system should be used in respect of such parking. Either two personnel travel in the same vehicle or two vehicles park relatively close together at synchronized times and the occupants move to and from the careers office together. Garages or parking spaces are not to be marked to indicate military usage, and wherever possible those "reserved" (but unmarked) spaces should be regularly exchanged with other "reserved" spaces.

9. **Building alarm system.** An alarm system is to be fitted to the careers office in such a way that it will allow staff to determine whether the building has been illegally entered before they themselves enter the building. Ideally the alarm indicator should be in a concealed location known only to the staff.

10. **Rolling grilles to cover windows and entrances.** Rolling grilles to cover windows and entrances should be considered for offices assessed to be at high risk from vandalism.

11. **Emergency exits.** Where practicable, a careers office is to have an emergency exit on a different side of the building from the main entrance.

12. **Outside sheds and storage areas.** Outside sheds and storage areas (to store refuse bins etc) are to be well-built and have substantial hard wood or metal doors and are to be secured by a 5-lever deadlock. All careers office equipment and aids should be stored in an internal store.

Personal Security Measures

13. Irish republican terrorists are likely to have targeted careers office personnel and vehicles by surveillance over a period of time, noting patterns of movement including timings and vehicles used. Careers personnel could unwittingly lead terrorists to vehicles parked nearby. To counter this surveillance, consideration is to be given to adopting the following counter measures where possible:

a. Personnel are to be especially vigilant and aware of the surveillance threat when arriving at and leaving the careers office. If suspicions are aroused, personnel should move immediately to a secure location and alert the civil police.

b. When arriving at or leaving the careers office, staff should consider the use of a "buddy" system to provide mutual support and visual cover for each other.

c. Routes to and from careers offices, whether on foot or by vehicle, should be varied.

d. Timings of arrival at and departure from careers offices should be varied.

e. Personnel should wear civilian clothes when travelling to and from careers office premises and make a conscious effort to blend in with the local civilian population.

Vehicle Security Measures

14. **General.** In the past, terrorists have exploited the vulnerability of careers office vehicle parking arrangements. To reduce this vulnerability the use of vehicles and their parking arrangements are to be kept under review and the guidance shown below should be implemented where feasible.

15. **Service vehicles.** If it is essential that they are used Service vehicles are to be parked within Service establishments whenever possible. They are only to be parked unattended in public places where it is unavoidable and, in such cases, they must be searched thoroughly prior to re-use.

16. **UVIED detection.** If the Service vehicle is fitted with a UVIED detection alarm system (such as TALOS), the alarm display unit is to be checked before attempting to enter or touch the vehicle. All drivers of vehicles fitted with UVIED detection systems are to be fully briefed on their operation before using the vehicle. Appropriate guidance has been issued to users.

17. **Civilianized military vehicles**.

a. The use of civilianized military vehicles in the vicinity of careers offices should be reduced to a minimum. Recruiting staffs should ensure that only those vehicles essential for the work of the careers office are held for use. The use of hire vehicles should be encouraged.

b. Every effort is to be made to avoid linking specific vehicles with careers offices. Consideration is to be given to the use of public transport by personnel travelling to and from work. Private vehicles should not normally be used. Long term lease or hire vehicles and/or civilianized white fleet vehicles should be regularly rotated.

c. Alternatively, consideration should be given to a system whereby careers office personnel are taken to and from work collectively by vehicles that do not remain at the careers office but operate from a secure location.

18. **Vehicle parking**. Where it is necessary to use vehicles in the vicinity of careers offices and to park them locally, consideration is to be given to the following measures:

a. Parking in a secure military establishment or, by permission, in a local police station (vehicle searches should still be carried out).

b. Public parking places are, where practicable, to be changed daily and an indirect route taken to and from the careers office.

c. Isolated and insecure sites, such as alleys, should be avoided.

d. Parking some distance (up to 15 minutes walking radius) from the careers office. Close parking will more easily enable terrorists to link vehicles to the office.

e. Every effort should be made, through the chain of command, to obtain lockable garages for careers office vehicles.

19. **Vehicle searching.** It is stressed that there is no substitute for comprehensive vehicle searching, whenever a vehicle, whether Service, civilianized or private has been left unattended, even in a locked garage. A search on a civilianized or private vehicle in a public place should be carried out as surreptitiously as possible to avoid indicating the Service connection. Under-vehicle search mirrors and torches are to be available at all careers offices.

Office Security Measures

20. **Liaison with police.** Good local contact should be maintained with the civil police, Service police or MDP. Inclusion on patrol routes of the police forces, where possible, should be requested, particularly at office opening and closing times. Inclusion in SVA, neighbourhood or other local watch schemes should be considered.

21. **Searches.** Guidance on counter terrorist search awareness is contained in Annex J. The outside and inside of careers office premises are to be comprehensively searched before occupation at the beginning of each working day and also at other irregular intervals. Where applicable, and possible, the start work check should include easily accessible flat roofs. These procedures are particularly important after weekends and public holidays. Office cleaners must not have access to the careers office before security sweeps have been completed.

22. **Office security procedures**.

a. Office furniture in public areas should not have shelves or drawers where IEDs could be left.

b. Irregular but frequent security sweeps are to be conducted.

c. Public access into the careers office should be restricted to one door only which is to be monitored by a member of staff.

d. Visitors to the careers office are to be identified and supervised whilst in the careers office.

e. Unattended doors must be locked whenever security measures dictate.

23. **Parking by the general public.** Where possible, parking by the general public should be restricted within 25 metres of the careers office through negotiations with local authorities by use of:

a. Double yellow lines.

b. Concrete or metal bollards.

c. Cones (that could cover a device) should only be used as a last resort.

24. If it is not possible to restrict public parking outside careers offices, the staff should be alert to any unusual activity in relation to vehicles and their occupants.

25. **Careers offices environs.** Exits and entrances are to be kept clear of debris and other items that could conceal an IED, including refuse bins and bicycles.

Security during Recruiting Activities away from the Careers Office

26. Careers staff undertake a wide range of duties away from the office, including:

a. Town or county shows.

b. Careers conventions.

c. School visits.

d. ATC/ACF/CCF/OTC/UAS, etc visits.

27. Much of this activity is, by its very nature, open to the public and pre-notified, if not publicized, before the event. Careers office staff should therefore be aware that these activities could provide terrorists with a means whereby they could be targeted. The provisions of paragraphs 07448 to 07469 (Security at Public Military Events) should, when applicable, be applied for all such events. In addition, the appropriate aspects of the following Annexes should be considered and acted upon:

a. Annex J to Section IV - Guidance on Counter Terrorist Search Awareness Security Measures.

b. Annex B to Section V – Guidance on Personal Security when Travelling.

This page intentionally left blank

ANNEX G TO SECTION IV TO CHAPTER 7

CIVIL POLICE CONTROL AND COORDINATION OF THE EMERGENCY SERVICES' RESPONSE IN THE EVENT OF A MAJOR TERRORIST INCIDENT

Command and Control

1. Dependent on the size and location of the incident, 3 levels of civil police command and control may be established:

a. **FCP.** The FCP will normally be the first control to be established by those nearest to the scene of the crime and responsible for immediate deployment and security. Under the command of the Incident Officer, the functions may vary depending on the siting of the Incident Control Room.

b. **ICP.** The ICP will control and co-ordinate the management of the incident, providing a central point of contact for all emergency and specialist services. The ICP will be the responsibility of an ICP co-ordinator and also under the command of the Incident Officer.

c. **Major Incident Control Room.** The need for such a control is dependent on the size of the incident. In some cases, even though there is a number of casualties all aspects of the operation will be co-ordinated through the ICP. However, with protracted incidents where there are ongoing manpower and logistical requirements, a major incident control room may be established to co-ordinate the overall response and provide facilities for senior command functions. The major Incident Control Room will be under the command of the Overall Incident Commander (OIC).

2. Whilst the rank of officers nominated may vary dependent on the individual force establishments, the following command functions will be necessary:

a. Overall Incident Commander (OIC) - Chief Officer.

b. Incident Officer - Divisional Commander.

c. Senior Investigating Officer - Detective Superintendent.

d. Major Incident Room Co-ordinator - Superintendent/Chief Inspector.

e. ICP Co-ordinator - Sub Divisional Commander.

3. Where forces adopt the GOLD, SILVER, BRONZE concept the following applies:

a. GOLD - Overall Commander.

b. SILVER - Incident Commander.

c. BRONZE - Sector Commander engaged on site.

4. As these command and control functions are established, the tasks associated with each will be progressively implemented. Invariably, however, initial responsibility after an incident will fall to the first officer to arrive at the scene who will act as Incident Officer, until replaced by a senior officer, and to the Divisional and Force Operations Rooms which will undertake the rapid mobilization of resources.

Initial Action by the First Officer at the Scene

5. The first officer at the scene will normally be a police constable. His immediate responsibility is to ensure that other emergency services are informed if they are not already in attendance. His priorities are to ASSESS and INFORM on the following:

a. Exact location of the incident.

b. Type of incident.

c. Hazards present and potential.

d. Access routes for emergency vehicles, turning routes etc.

e. Casualties.

f. Emergency services present and required.

Action by the Divisional/Sub Divisional Control

6. Action by the Divisional/Sub Divisional Control, if applicable, is as follows:

a. Inform the Force Ops Room.

b. Direct the nearest officer to the scene to assess the situation.

c. Inform the senior officer on duty who will attend and assume the role of Incident Officer.

d. Inform the Divisional Commander or his Deputy.

e. Deploy personnel as directed by the Incident Officer.

f. Commence a log and co-ordinate the Divisional Response.

g. Maintain liaison with the Force Operations Room.

Action by the Force Operations/Control Room

7. Upon receipt of information that an incident has occurred, the Duty Officer in the Force Operations Room/Centre/Control is responsible for instigating the mobilization of the emergency services, specialist agencies such as EOD, police manpower and for establishing communications with the first officer at the scene.

8. Aide memoire procedure sheets are normally prepared in accordance with individual force mobilization plans and are immediately taken into use should an incident occur. These procedure sheets include information for the mobilization or implementation of the following if required:

a. Other emergency services.

b. FCP.

c. Traffic control.

d. Divisional Command.

e. Divisional personnel.

f. Local authority.

g. Major incident control vehicle and equipment.

h. Hospital documentation team.

i. Scene photographers.

j. Major Incident Control Room staff.

k. Press liaison.

Scene Management

9. The immediate and overriding responsibility of the emergency services at the scene of an incident is to save life. To this end, the Fire and Ambulance Services must be afforded the opportunity to utilize their training and experience. The prime responsibility of the Incident Officer is to facilitate the deployment of the emergency/specialist services.

10. During the rescue phase, the civil police co-ordinating role is vital and the Incident Officer, who is the link to every other police control, will undertake a preliminary reconnaissance and determine what action has been taken to establish:

a. An ICP.

b. Security at the scene.

c. Traffic control.

d. Casualty clearance.

e. Property team.

f. Hospital documentation team.

g. Mortuary facilities.

h. Liaison with other emergency/specialist services.

11. When it becomes apparent that no further life can be saved other considerations take precedence:

a. Preservation of the scene of crime.

b. Recovery of the deceased.

c. Investigation.

d. Identification of the deceased.

Incident Control Post

12. Operational command will be at the ICP. Initially, the first police vehicle at the scene will become the FCP/ICP. Thereafter, other options for the ICP may be considered. The ICP should have facilities for radio and telephone and should be sited such that it is:

a. Safe.

b. Accessible.

c. Conspicuous.

d. Secure.

Security and Preservation of the Scene

13. **Cordons.** The civil police will establish 2 cordons:

a. **Outer Cordon.** To seal off an extensive area and prevent unauthorized access.

b. **Inner Cordon.** To provide immediate security of the "scene of crime".

c. **Cordon Personnel.** Normally police officers deployed in cordons will be divided into units, each under the command of a Sergeant and responsible for a fixed section of the boundary. A senior police officer will normally be

appointed to oversee the maintenance and resourcing of the cordons through the ICP.

14. **Media Liaison.**

a. Terrorist incidents generate intense media interest. Representatives of the press and television may be at the scene of an incident as quickly as the emergency services.

b. The civil police will make provision for media liaison as follows:

(1) **Press Liaison Officer.** May be an officer nominated by the incident officer, a member of the Force Press Liaison Section or a designated officer, who will be directed to the scene and be responsible for the release of information.

(2) **Press Liaison Point**. An area will be designated for exclusive use by the media. Accredited members of the press will be directed to this area.

15. **Traffic Control.**

a. Immediate action will be taken by the civil police to ensure free passage for emergency traffic to and from the scene.

b. Whenever possible, a one way system will be implemented to ensure the rapid attendance of emergency vehicles at the scene and facilitate the evacuation of casualties to hospital.

c. **Marshalling area.** An area suitable for accommodating a large numbers of vehicles will normally be designated a marshalling area for those resources not immediately required at the scene. Vehicles at the scene will not be allowed to remain at the scene.

d. **Diversions.** Diversions will be established if necessary to divert all non essential traffic from roads leading to the incident.

16. **RVP.** As soon as practical, all civil police resources attending the scene will be directed to nominated or pre-designated RVPs. An officer will be appointed to run the RVP. The function of the RVP is as follows:

a. Maintain a log of incoming civil police resources.

b. Inform the ICP of their availability.

c. Brief officers attending the scene.

d. Issue equipment.

e. Log details of resources leaving the RVP to be deployed.

f. Direct resources to a marshalling area.

Casualty Clearance

17. The civil police will liaise closely with the Ambulance Service and the MO in charge at the scene. To co-ordinate the removal of the injured, the Ambulance Service after consultation with the Emergency Services as to location, routing and signing will set up:

a. Casualty Receiving Station.

b. Ambulance Loading Points.

c. Ambulance Parking Point (Marshalling Area).

d. Ambulance Control Point.

Evacuees

18. An officer with local knowledge will normally be the designated Evacuation Officer. He will be responsible to the Incident Officer for all evacuations.

19. Suitable buildings/covered areas will be identified as Evacuation Assembly Points and signed as such. All evacuees will be directed there for transport to "Rest Centres" run by the local authority.

Investigation

20. After an incident, the overall Incident Commander will appoint a Senior Investigating Officer to collate evidence for:

a. The Coroner.

b. Any Inquiry.

c. Criminal Proceedings.

21. Teams of officers under the command of the Senior Investigating Officer will be responsible for evidence gathering from the scene and for interviewing witnesses as follows:

a. Survivors.

b. Eyewitnesses.

c. Emergency Services personnel.

d. Technical witnesses.

e. Background witnesses.

f. Identification witnesses.

22. Once the rescue and victim recovery phases of the operation are complete, an extensive search will be undertaken to recover items for evidential purposes. Police personnel trained in search techniques will be used for the task.

This page intentionally left blank

APPENDIX 1 TO ANNEX G TO SECTION IV TO CHAPTER 7

ACPO EMERGENCY PROCEDURES TERMINOLOGY

Approach Path. Route taken from the inner cordon entry point to the scene of the crime or seat of explosion.

Casualty. Any person who is directly involved or is affected by an incident, i.e. survivors, deceased, evacuees.

Casualty Bureau. Central contact and information point established by the civil police for all records and data relating to casualties.

Controlled Area. The area contained by the outer cordon.

Cordons

> **Inner cordon.** Surrounds the immediate scene of crime and provides security for it.
>
> **Outer cordon.** Seals off an extensive area to which unauthorized personnel are not allowed access.

Cordon Entry Point. Point at which authorized personnel gain entry to the inner cordon. The entry point is normally controlled by the cordon officer/commander or nominated cordon personnel.

Cordon Officer/Commander. Responsible to the incident commander for the siting, deployment and management of the inner and outer cordons.

Designated Receiving Hospital. Those hospitals identified by the Regional Health Authority as suitable for receiving multiple casualties.

Evacuation Assembly Point. Area or building to which evacuees are directed before subsequent transportation to a rest area.

First Officer to the Scene. First civil police officer directed to the scene of an incident to assess and inform.

FCP. The control point nearest to the scene of the incident responsible for immediate deployment and security.

ICP. The point from which the management of an incident is controlled and co-ordinated. The central point of contact for all specialist and emergency agencies on site.

IC SILVER. The civil police forward operational commander, controlling and co-ordinating the police operation within the controlled area and responsible to the overall civil police incident commander. The Service equivalent is the establishment incident commander, normally the Duty Officer.

Major Incident Control Room. Established by the civil police in protracted incidents to co-ordinate overall response, dealing with ongoing manpower and logistics requirements and providing facilities for senior command functions.

OIC GOLD. The designated civil police chief officer who assumes command of the operation as a whole. The Service equivalent is the senior officer, i.e. the HOE.

Police Call Back. Procedure whereby the civil police call back to confirm an initial call is bonafide and subsequently maintain an open line to the establishment main guardroom or ICP.

PST. Civil police search team.

Press Liaison Officer. Civil police representative responsible for the initial release of information from the scene of an incident.

PLP. Area adjacent to the incident scene designated for the exclusive use by accredited media representatives and through which official press releases occur.

Red Line Telephone. The dedicated telephone line for incoming calls only, which is used by the civil police to call back and remains open thereafter.

RVP. Point to which all resources arriving at the outer cordon are marshalled, directed for logging, briefing, equipment issue and deployment further forward if required.

RVP Officer. Civil police officer responsible for the routine of the RVP.

Rest Centre. Building designated by the local authority for the temporary accommodation of evacuees.

Senior Investigating Officer. The senior detective officer appointed by the OIC to assume responsibility for all aspects of the civil police investigation.

ANNEX H TO SECTION IV TO CHAPTER 7

GENERAL PRINCIPLES OF INCIDENT MANAGEMENT

General

1. Although each incident will be different in nature, it is possible to lay down certain principles that will be common to all.

Evacuation

2. Evacuation of a building or area may become necessary as a result of the discovery of a suspicious item, a warning, or in consequence of an explosion. Once ordered, the evacuation must be effected quickly, but in a controlled and co-ordinated fashion.

3. **Evacuation plans.** Evacuation plans should be prepared in advance, publicized and rehearsed on a regular basis. The evacuation itself should be controlled by a nominated person acting on behalf of the overall incident commander.

4. **Area to be cleared.** The area to be cleared will depend upon the nature of the incident:

a. **Suspect IEDs**

(1) For a device placed by hand, at least 100m radius.

(2) For a suspect vehicle or larger item, at least 400m radius.

b. **Explosion.** At least 100m from the extremity of the scene of the explosion.

c. **Mortar blinds.** At least 200m from any unexploded mortar round.

5. The size of the area will also be influenced by topography and secondary hazards, such as fuel or a large expanse of glass. Due consideration should also be taken of likely blast effects.

6. **Method of evacuation.**

a. **Direction.** Starting at the scene of the incident, work outwards. In the case of suspect devices, avoid evacuating past the object or being in line of sight.

b. **Cascade.** To save time, when evacuating buildings adopt a cascade system where members of the guard alert a small number of nominated occupants, who are then responsible for arousing and evacuating other personnel present, releasing the guard to move on to other buildings or tasks.

c. **Inform.** Personnel responsible for evacuation should tell evacuees:

(1) Why the evacuation is taking place.

(2) If a suspect device is involved, its location.

(3) Where to go, including exit points and the route to, and location of, the Evacuation Assembly Point. Routes should be chosen to avoid confusion or bunching and that avoid potential hazards such as plate glass or windows.

d. **Action by Evacuees.** Before exiting the area, evacuees should:

(1) Secure all protectively marked material.

(2) Carry out a quick visual search of their immediate work and living areas.

(3) Open windows, leave lights on and doors open.

(4) Leave the area and proceed to the evacuation assembly point.

(5) Take personal belongings such as coats, handbags, briefcases, etc with them.

(6) Evacuees leaving living accommodation at night should take a pre-package evacuation bag containing overnight kit.

e. **Clearance check.** A system should be established for ensuring that all buildings and areas within the potential danger area have been evacuated and cleared.

f. **Evacuation assembly point.**

(1) Evacuation assembly points should be carefully sited. They should be sufficiently far from the scene of the incident and in open areas that may be easily checked for IEDs. Car parking areas containing vehicles should be avoided.

(2) Before evacuees assemble, the immediate area should be checked for possible secondary IEDs by a nominated member of the guard.

(3) There should be clearly established assembly point procedures and a person, preferably of at least SNCO rank or AO grade, should be nominated to control and marshal evacuees and check on nominal rolls.

(4) Establishment should avoid the regular and routine use of the same assembly point as part of exercises or in response to threatening telephone calls.

Cordon

6. The cordon area may be divided into the inner and outer cordons.

a. **Inner cordon.** Once clearance and evacuation has commenced, a cordon must be placed around the scene of the incident to isolate the danger. A suitable Cordon Entry Point should be selected, through which all authorized personnel enter the danger area.

(1) **Size.** The size of the area to be cordoned will depend upon the nature of the incident, but it should encompass the entire danger area and in particular the area that has been cleared and evacuated. It is easier to contract a cordon at a later stage than to expand it.

(2) Cordon positions

(a) Should be carefully chosen and sited by a nominated cordon commander.

(b) Should be situated at the edge of the cleared area.

(c) Should avoid obvious positions where secondary devices could have been placed.

(d) Should be checked by cordon personnel prior to occupation for secondary devices.

(3) **Cordon commander.** A cordon commander should be appointed to oversee the management and deployment of the cordon. Ideally, the cordon commander should be located at the Cordon Entry Point.

(4) **Cordon personnel.** Sufficient numbers of cordon personnel should be deployed to ensure complete security of the inner cordon area. All obvious access routes into the cordon area should be manned.

(5) **Barriers.** To save manpower, physical barriers may be erected to block access points. Tape may be used to delineate the cordon area.

b. **Outer cordon.** An outer cordon may be deployed to prevent unauthorized access to the Incident Area and to create a controlled environment in which the emergency services may operate. Outside Establishment perimeters, the outer cordon is a civil police responsibility. Inside a large establishment, if sufficient personnel are available, an outer cordon may be deployed to assist control at the scene.

Control

7. The following command and control elements should be established in response to any incident:

a. **Incident commander.** The incident commander is responsible for the initial command and control of the incident, until handing over to the civil police incident commander. The incident commander should:

(1) Conduct an appreciation of what has occurred and what action needs to be taken.

(2) Initiate and supervise follow up actions, giving clear directions to those involved.

(3) Ensure that full briefings are given to the civil police, EOD, Command staffs, and Focal Point depending upon local SOPs.

(4) Establish an Incident Control Post (ICP).

Once control of the incident has been passed to the civil police incident officer, the incident commander should remain with him to act as a liaison officer.

b. **ICP.** An ICP should be established at an early stage and should become the focal point for the control and co-ordination of follow-up action. The ICP should be:

(1) The point of contact for specialist agencies and the emergency services.

(2) Located in a building equipped with telephones and radios and may often be a custom built command post such as a control room or guard room.

Alternative ICP locations should be identified for activation, should the primary ICP be located in a potential danger area.

c. **Incident box.** An incident box should be prepared and pre-stocked with the following items:

(1) Establishment maps, plans and aerial photographs.

(2) Road signs.

(3) Directional signs.

(4) Log books, message pads and stationery.

(5) First aid kit and minor rescue equipment.

(6) High visibility vests for key personnel.

(7) Torches.

(8) Loud hailer.

(9) Cordon tape.

d. **Forward Control Point (FCP).** An FCP should be established at the edge of the cordon and should become the focus of activities at the scene itself. Security of the incident and deployment of personnel should be exercised from the FCP.

e. **Rendezvous Point (RVP).** The RVP is the point to which the civil police, EOD and other emergency services will report before being directed forward to the ICP or FCP. The RVP should:

(1) Be clearly signed and marshalled by nominated personnel.

(2) Have adequate access and parking space for a large number of vehicles.

f. **Briefing**

(1) Once control of the incident scene has been established an area should be nominated for briefings to take place. Ideally, the briefing area should be located close to the ICP.

(2) A detailed briefing should be prepared for civil police and EOD, detailing the circumstances of the incident and all actions that have been taken.

Terminology

8. Standard ACPO Emergency Procedures Terminology is detailed at Appendix 1 to Annex G.

This page intentionally left blank.

APPENDIX 1 TO ANNEX H TO SECTION IV TO CHAPTER 7

ACTION UPON DISCOVERY OF A SUSPECTED IED

General

1. If a suspicious object is discovered that could be an IED and its presence cannot be readily explained it is to be treated as a genuine device and must not be touched or moved. Either an object is suspicious or it is not. ***There is no such thing as a possible suspect IED.***

2. Attempts to establish ownership of the object or the identity of the person who placed it should continue, but should not take precedence over immediate response drills.

Immediate Response Drills

3. **Phase One - Confirm.** Confirm the presence of a suspicious object.

   a. If a reliable witness reports a suspect IED inside the establishment perimeter accept the information. Do not wait until someone has been to check. Gather all available information, including the exact nature of the device and its precise location.

   b. If a patrol or search team discovers a suspect IED they should immediately withdraw to cover and send an incident report to the security control room.

4. **Phase Two - Clear.** Having confirmed the presence of a suspect IED, all personnel should be evacuated from the surrounding area. The size of the area to be cleared will depend upon the nature and size of the object, together with any secondary hazards that may be present; as a guide the following distances should be observed:

   a. Device placed by hand - at least 100m.

   b. Suspect cars - at least 400m.

   c. Suspect vans or lorries - at least 400m

5. **Phase Three - Cordon.** A cordon should be established around that area that has been cleared, to prevent personnel entering into the danger area.

6. **Phase Four - Control.** A nominated incident commander should exercise control over the incident until relieved by a civil police incident officer.

7. **Concurrent Actions.** In addition to controlling activities at the scene, the incident commander should:

a. Continue attempts to identify the owner or person who placed the object. Consideration should be given to making suitable public address system broadcasts.

b. Hold all available witnesses at some suitable location for interview by the civil police and EOD. It is particularly important that the person who discovered the device, or any other person who has closely observed it, should be present.

c. Issue suitable briefings to the civil police, PSyAs and Command security staff, local security unit and Focal Point as may be appropriate.

APPENDIX 2 TO ANNEX H TO SECTION IV TO CHAPTER 7

ACTION SHOULD AN IED EXPLODE

Explosion after Evacuation - No Casualties

1. The Cordon should be maintained. Access to the area of the explosion is to be restricted to specialist personnel, e.g. EOD and the civil police.

2. The Fire Service may be required to fight any fires that may threaten undamaged buildings provided this can be achieved without putting personnel at risk from other IEDs.

3. A full telephone Incident Report should be sent to the following:

   a. The civil police if they are not yet in attendance.

   b. PSyAs and Command security staff, local security unit and Focal Point (depending on SOPs).

Explosion with Casualties

4. The priority is to save life and search for and evacuate casualties.

5. Despite the understandable willingness of many personnel to approach the area of an explosion and provide help, control must be exercised over rescue efforts.

   a. The minimum number of personnel should be employed in the search for casualties in order to minimize the risk from further IEDs, falling masonry and fire.

   b. Those rescue personnel approaching the seat of the explosion should move in on a designated approach path and exit by the same route. This will reduce the risk from other IEDs and minimize the possibility of contaminating or destroying evidence in the debris.

   c. Bodies should be left in situ and should not be touched or covered.

   d. Establishment contingency plans must include casualty evacuation arrangements and provision made for rescue equipment such as stretchers, ropes, hydraulic jacks, props and heavy lift gear to be available if required.

   e. A casualty list should be prepared and passed up the chain of command in accordance with local SOPs. "KINFORM" actions should be taken without delay.

This page intentionally left blank.

APPENDIX 3 TO ANNEX H TO SECTION IV TO CHAPTER 7

ACTION IN THE EVENT OF A MORTAR ATTACK

Immediate Response Drills by Gate Guards or Patrols

1. It is likely that gate guards or patrols will be the first to be aware of a mortar attack. Their immediate response should be to activate the attack alarm or relay a message to the security control by radio.

2. The gate guard or patrol is then to take cover and attempt to count the reports from the base plate and the reports of bombs exploding. This information is to be reported without delay to the Security Control with details of the area attacked and the direction from which the mortars were launched, if this can be assessed.

Immediate Response Drills by the Guard Commander

3. If necessary, activate the attack alarm.

4. Take cover.

   a. Inform the following by sending a radio or telephone incident report.

      (1) The civil police using 999. Request the civil police to:

         (a) Ask for EOD assistance.

         (b) To nominate a Rendezvous Point (RVP); this should be outside the establishment perimeter.

      (2) PSyAs and Command security staff, local security unit and Focal Point (depending on local SOPs).

   b. Keep personnel under cover. There is no laid down time for remaining in cover. However, the commander on the spot should anticipate a 2 phased attack that could last 15 minutes.

   c. Once a safety period has elapsed deploy a search team to:

      (1) Locate blinds.

      (2) Locate casualties.

(3) Locate the base plate.

(4) Identify a safe evacuation route for other personnel.

d. Once the base plate has been located, the area around the base plate to a radius of 300m and the area under the flight path and the impact area to a radius of 100m must be cleared of personnel and cordoned off. Ensure that no attempts are made to touch the base plate or any blinds.

e. Once casualties have been dealt with and the area secured, the control drills that are to be followed are the same as those for an IED.

Immediate Response Drills by other Personnel

5. On hearing the attack alarm, the sound of a mortar firing or the detonation of a mortar round, all personnel are to take cover immediately by:

a. **Inside Buildings.** Lying on the floor or ground. Where possible this should be done away from windows and preferably under some form of hard shelter such as tables, desks, beds or internal corridors.

b. **Outside Buildings.** Seeking cover immediately wherever they can and then moving as quickly as possible to the shelter of a building as soon as the alarm or explosions stop.

c. **Vehicles.** Vehicles should not be abandoned obstructing roads.

6. Personnel should remain under cover unless:

a. They are ordered to move.

b. They are aware of an unexploded bomb or blind nearby.

c. They are aware of a casualty requiring assistance.

d. The all clear sounds.

7. Personnel who are aware of the existence of unexploded bombs or blinds are to inform the Incident Control Point immediately.

APPENDIX 4 TO ANNEX H TO SECTION IV TO CHAPTER 7

ACTION IN THE EVENT OF A TERRORIST SHOOTING ATTACK

General

1. Armed personnel coming under fire from a terrorist gunman within establishment perimeters should respond positively, operating within the authorized and relevant ROE JSP and according to establishment plans and orders.

Immediate Response Drills

2. **Return fire.** If the conditions specified in the relevant ROE JSP are met and fire is returned, only single aimed shots should be used.

3. **Initial contact to the main guardroom/security control room.** An initial contact report should be made to the Security control room including:

   a. Contact location.

   b. Information on position of intruders.

   c. Casualties.

4. **Clear the area.** Take whatever follow-up action may be necessary to clear and secure the area and ensure there is no further threat.

5. **First aid.** Apply first aid to any casualties and call an ambulance.

6. **Hot pursuit.** Action to pursue and apprehend the gunman can only be taken within the provisions of JSP 385. NB, This does not apply to Scotland. If hot pursuit has to take place beyond establishment boundaries, consideration must be given to the danger posed to the general public and the ability of the local police to respond. If such action is successful, the gunman should be arrested and held until handed over to the civil police.

7. **Inform civil police.** Inform the local civil police (and the MDP or Service police if stationed at the location), notify the local security unit, PSyA or Command security staff. All relevant police forces should be informed of the precise nature and location of the incident, although the primacy of the civil police in the investigation must be respected. In addition, it should be made clear whether there are other suspects or vehicles and, if so, full descriptions given where possible.

Subsequent Action

8. **Clearance.** Check the establishment for any devices. Do not touch discarded weapons or equipment. Be aware of possible booby traps.

9. **Cordon.** Isolate the scene and place a cordon around the firing point area and the contact point until the civil police arrive. Thereafter, act on their instructions.

10. **Control**

a. Maintain a log of the sequence of events for a subsequent full report and for use at any subsequent enquiry.

b. Establish a Rendezvous Point (RVP) and an Incident Control Point/Forward Control Point (ICP/FCP).

c. Hand over control to the civil police.

11. **Witness information.** Ensure that any witnesses, military or civilian, do not leave the scene before the police arrive. If a Service person or MDP officer has carried out the shooting, ensure that the individual remains under escort until the civil police arrive. (The individual who fired is likely to be in a state of shock and should, if possible, be escorted to a nearby building rather than required to remain exposed at the scene).

12. **Evidence.** Take action to preserve all evidence in the immediate area as well as at the scene (including spent ammunition cases). The scene of the incident should not be interfered with except for safety reasons until the civil police are present. Weapon(s) should not be touched until a police authorized firearms specialist is in attendance.

13. **Reporting.** Inform PSyAs and Command security staff, local security unit and Focal Point as required by local SOPS.

14. **Brief personnel.** Brief all Service personnel and their families living in the immediate area on:

a. What has happened.

b. Any further threat.

c. What action, if any, to take.

15. **Press statement.** HOE should, if necessary, issue a short press statement confirming an incident has taken place. A standard statement for this purpose is provide below. HOE should liaise with the police and their Command Media Ops staff over the further release of public information. No personal details of those involved should be given. No other personnel should make any statement to the media.

Standard Press Release Confirming an Incident has Occurred

AT (time) TODAY AN INCIDENT OCCURRED AT (location) WHICH RESULTED IN (number) PEOPLE, INCLUDING (number) OF SERVICE PERSONNEL BEING SHOT. THE INCIDENT IS NOW THE SUBJECT OF A CIVIL POLICE ENQUIRY. ANY FURTHER QUERIES SHOULD BE ADDRESSED TO (name) CONSTABULARY.

Possible Police Action following a Terrorist Shooting Incident

16. Personnel who become involved in a terrorist shooting incident should be advised of the possible civil police action following such an incident. Despite what may appear to the layman to be a laudable, brave act committed by a person in accordance with the Rules of Engagement, the civil police have a duty fully to investigate the incident and establish the circumstances. To fulfil this duty, it is possible that the civil police may caution and detain an individual in the pursuit of their enquiries. This of itself does not mean that the individual is guilty of an offence. Any individual in this situation has the right to independent legal advice and obviously has a right to reserve a defence.

17. In normal circumstances an individual should provide information that may have an immediate bearing on the apprehension of terrorists, the saving of life or the prevention of damage to property.

Support to Personnel following a Terrorist Shooting Incident

18. Obtain the services of a solicitor to act for the individual who has carried out the shooting.

19. Appoint an officer, to assist the individual concerned.

20. Obtain the advice and assistance of the SMO or retained Civilian Medical Practitioner to ensure that the person responsible for the shooting is assessed for the effects of stress or any other medical condition resulting from the incident.

This page intentionally left blank

APPENDIX 5 TO ANNEX H TO SECTION IV TO CHAPTER 7

ACTION IN THE EVENT OF A PROXY BOMB ATTACK

General

1. Proxy bombs can explode any time after being delivered, immediate response drills therefore must be implemented quickly.

2. The driver of a proxy bomb may well be acting under duress. The individual must be handled firmly but politely and is a potentially valuable witness.

Immediate Response Drills

3. **Action by the gate guard.**

a. Raise the alarm.

b. Attempt to persuade the driver to drive the vehicle to a place where the explosion may cause less damage. Areas to which vehicles can be driven should be a previously designated part of the establishment identified in the contingency plan.

(1) Do not try for more than 15 seconds.

(2) Do not use physical force.

(3) Do not drive the vehicle yourself.

(4) Do not get into the vehicle yourself.

c. Detain the driver and move to safety.

4. **Action by the guard commander.**

a. Sound the alarm.

b. If necessary, move to a safe area or alternative ICP.

c. Clear and evacuate by deploying members of the guard to evacuate personnel quickly from the danger area (minimum 400 metre radius) to an Evacuation Assembly Point that may be outside the establishment perimeter.

d. Ensure the Evacuation Assembly Point is checked for secondary IEDs.

e. Inform the civil police using 999 and send a telephone Incident Report.

f. Inform the PSyA or Command security staff, local security unit and Focal Point depending on local SOPs.

g. Place an inner cordon round the danger area to a minimum radius of 400m.

h. Establish an RVP and ICP/FCP.

i. Hand over to the civil police.

ANNEX I TO SECTION IV TO CHAPTER 7

AIDE MEMOIRE FOR EVENT SECURITY OFFICERS (ESOS)

1. This Aide Memoire is designed primarily for the use of non-specialist ESOs nominated to cover PMEs off MOD property. ESO responsibilities for PME on MOD property should be overseen by the ESyO.

Prior to the Event

2. **At Least 2 months in advance.** Start preparing the proforma at Appendix 1 to ensure its arrival with the civil police HQ contact officer and the other addressees at least **6 weeks** before the event.

3. **Five weeks before the event.** Contact the civil police to discuss detailed security arrangements. Points should include:

a. Searching and securing of the venue (including any Service changing accommodation) prior to the event.

b. Searching and securing of the arrival, debussing and embussing point(s) of Service participants and the immediate approaches to those points.

c. Protection of transport.

d. Control of access to the venue from the moment any search beings or, if no search is required, when it is opened to the public until all participants are dispersed. (Unauthorized personnel should not be admitted once the clearance search has been started).

e. Monitoring and control of approaches to the venue immediately prior to, during and after the event until all participants have dispersed.

f. The roles of Service personnel provided for security duties such as the protection of transport.

4. **Subsequently.** Co-ordinate organization of Service aspects of the security plan. Points should include:

a. **Transport.**

(1) Anonymous or is the Service identity essential to the purpose of the PME, e.g. a recruiting display?

(2) Full details passed to civilian transport firm as late as possible.

(3) Multiple as opposed to single vehicles e.g.: personnel coming from different locations.

b. **Dress.**

(1) Anonymous for travel if relevant but see 4a(1) above.

(2) Arrange changing accommodation at the venue.

c. **Security personnel.** Ensure that unit personnel are organized to meet the number agreed with the civil police. If other support was requested ensure it is being provided.

d. **Communications.** Confirm what system is to be used.

5. **Shortly before the event.** Brief all personnel on the general security plan ensuring that:

a. Participants understand the need for alertness and vigilance.

b. Security personnel fully understand their duties.

On the Day of the Event

6. **Briefings.** Re-brief personnel as necessary.

7. **Oversee the deployment to the event.** This should include:

a. Checking of personnel and kit onto transport.

b. Paying particular attention to arrival, debussing and entering the venue.

8. **On arrival.** Contact the senior civil police officer on arrival and introduce your security personnel. If possible, together with the senior civil police officer, detail them to their duties.

9. **During the event.** Visit your security personnel to ensure all is well.

10. **After the event.** Ensure that, in accordance with the overall civil police plan, your security personnel remain on duty until all Service personnel are withdrawn.

11. **In the event of an incident.** In the event of an incident assist the senior civil police officer, where you can, in handling the matter.

12. **Post event action.** If any aspect of the security plan was not satisfactory, inform the chain of command.

APPENDIX 1 TO ANNEX I TO SECTION IV TO CHAPTER 7

NOTIFICATION OF A PUBLIC MILITARY EVENT (PME) IN GB

1. Military Reference….....……..Date.....….....

To: Civil Police Force HQ…….....….....….....

Local Sy Unit/RAF P&SS/MI Sect ..... (2 Copies)

Command SyO.....…….....

Army Division/District HQ .....…….....….....

Army Bde HQ...….....…….....….....

From:

2. Unit (Full Address).....…….....

.....….....…….....……..…

.....……

.....……

3. Telephone Number.....Offr IC tel no…….....…..

Fax Number.....Mobile tel no….…….....….....…

4. Date of Event…….....Event Timings

Start.....….....….……...…

Finish.....…...……..…

Unit time of Arrival.....Unit Time of Departure.….....…

Date of Leaving.....……..

5. Any rehearsal details (include dates/timings, numbers, recces etc).....

.....…….....

.....

(If less than 6 weeks notice is given the event may not be policed)

6. Full Name and Address of Venue:.....

.....

.....

.....

.....

7. Summary of Previous Use (incl dates)….....

.....

.....

8. Description of Event (e.g. Concert/Parade)…....

.....

.....

.....

9. **If a March or Parade:**

a. Form Up (Start Point and time).....

.....

.....

.....

b. Route (include map showing assembly area).....….....

.....

.....

.....

.....

c. Location of Dais..…….....

.....

d. Parade/March ends at (*Location/Time)*:…….....….....

.....……..

10. Numbers participating:..... Expected numbers of public…….....

11. Number of Service Personnel for Sy duties.....…….....

12. Overall Event Organizer....…….....……

a. Contact tel no.....……

b. Sponsor…….....……..

Contact tel no.....……..

d. Officer in Charge of Event.....……..

Mobile tel no....….....……

13. Event Security Officer (ESO):

a. Before the Event.....……..

b. At the Event.....……

14. Transport Arrangements:

a. To be used.....…….

.....……..

.....……..

.....……..

b. Parking Arrangements.....…….....

.....……..

.....……..

.....……..

c. Vehicle Guarding Arrangements.....……

.....……..

.....……..

.....

.....

.....

15. Accommodation plans (Changing or overnight (hotel etc))..... .....

.....

.....

.....

16. Publicity:

a. When was the Event publicized and how?.....

.....

.....

.....

b. Follow up publicity.....

.....

.....

c. Terrorist incidents involving this Unit.....

.....

.....

17. Details of VIPs attending:

Rank/Name	Appointment
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....
.....	.....

....

18. Any other details (Weapons involved etc).....

.....

.....

.....

.....

.....

19. Dress for event.....

.....

.....

.....

.....

Signed..... Name/Rank/Appt.....

Enclose PME Acknowledgment Slip (APPENDIX 2) and s.a.e addressed to unit requiring receipt

***(when completed consider upgrading protective marking)**

This page intentionally left blank

APPENDIX 2 TO ANNEX I TO SECTION IV TO CHAPTER 7
PME Acknowledgement Slip

(to be completed by appropriate Civil Police Force HQ)

1. To: .....

2. From: .....

3. Acknowledgement of notification of Public Military Event on Date.....

   Reference..... Venue.....

4. Receipt of your Proforma is acknowledged: (Delete as applicable)

   a. There are no security objections to the event taking place.

   b. It is advised the event should not take place.

5. The Police response will be as indicated below: (Delete as applicable)

   a. A search will be conducted and full Police cover will be given throughout the Event.

   b. A search will be conducted. However, on completion of the search, the military are requested to undertake responsibility for security at the event.

   c. The event has been noted and local Police Officers have been informed.

   d. No cover will be provided by the Police.

   e. A decision as to Police response is yet to be made.

6. Your Civil Police contact for the security arrangements for the event is:

   a. Name and Rank .....

   b. Civil Police Station .....

   c. Telephone number .....

Signature..... Date ……

Police Contact telephone number in case of emergency ….....

This page intentionally left blank

APPENDIX 3 TO ANNEX I TO SECTION IV TO CHAPTER 7

NOTIFICATION OF A PUBLIC MILITARY EVENT OVERSEAS

To:

HQ Comd)

UK Support Unit (NATO HQ)) as appropriate – see paragraph 07465

British Embassy/High Commission)

From: Reference:

1. **UNIT** (Address and telephone number including BT dialling code):

2. **DATE OF EVENT AND ON-SITE REHEARSALS** (If less than 6 weeks state reason for late notification):

3. **LOCATION OF EVENT**

   a. **Full details of venue:**

   b. **Brief summary of previous use of venue** (Including dates):

4. OUTLINE OF EVENT AND NATURE OF SERVICE INVOLVEMENT

   a. **Type of activity [(1)]:**

   b. **Numbers participating:**

c. **Expected number of spectators/audience/attendance:**

d. **Number of Service personnel dedicated to security duties in attendance:**

e. **Details of involvement/participation of other Services:**

5. **PERSONALITIES** (Names and contact numbers of the following):

a. **Overall event organizer** (If Service personnel are participating in a joint activity with civilians):

b. **Local sponsor, if appropriate** (e.g. Theatre manager):

c. **Unit person in charge at the event:**

d. **Event Security Officer** (ESO) (Responsible for civil police liaison and security organization - to include telephone numbers)

(1) **Before the event** [(2)]:

(2) **At the event** [(2)]:

e. **Overall ESO** (If other Service units are involved in the event) [(3)]:

6. **TRANSPORT ARRANGEMENTS**

a. **Transport to be used:**

b. **Parking location(s) throughout the total activity associated with the event** (e.g. rehearsals, overnight and during the event itself):

c. **Proposed guarding arrangements** (If not parked in a secure Service establishment or civil police station):

7. **TRAVEL ARRANGEMENTS**

a. **Outward journey.**

(1) **Method of travel with flight/sailing number:**

(2) **Arrival location with date and time:**

b. **Return journey.**

(1) **Method of travel with flight/sailing number:**

(2) **Departure location with date and time:**

8. **ACCOMMODATION ARRANGEMENTS**

a. **Changing accommodation:**

b. **Overnight accommodation address** (If civilian, the date of booking and confirmation that the reservation was made without reference to the Services):

9. **PUBLICITY**

a. **When the event was first publicized and how:**

b. **Follow-up publicity with dates** (e.g. regional newspaper coverage and local posters):

c. **Brief details of any previous terrorist incidents involving the unit:**

10. **DETAILS OF VIPs ATTENDING THE EVENT**

NOTES:

(1) Duty (Include details of type of activity, i.e. marching band, concert band, display team etc). Service, community, charity or fee-paying engagement.

(2) Ideally these are the same person.

(3) This may be decided subsequently in conjunction with the other Services if appropriate.

(When completed, consider upgrading protective marking)

APPENDIX 4 TO ANNEX I TO SECTION IV TO CHAPTER 7

OPEN DAY SECURITY PLANS

1. The style, format and structure of the open day security plan will be dictated by local circumstances; however, it should contain the following essential elements:

a. The composition of the security organization and command and control arrangements, including the location and function of the Joint Security Control Room.

b. Detailed plans depicting:

(1) The geographical and physical layout of the establishment, including the division between public and non-public areas.

(2) The location and arrangement of key elements of the open day, to include the crowd line, car parks, static equipment displays, VIP and Service enclosures, trade and exhibition stands etc.

(3) The location of access gates and physical barriers, including the erection of temporary obstructions and fences.

c. Access arrangements to both the public and non-public areas, including arrangements for the checking and searching of vehicles where necessary.

d. Vehicle parking arrangements, including arrangements for staff, exhibitors and traders, VIP guests and establishment personnel.

e. Pass systems and ticketing arrangements.

f. Security tasks and assignment of forces.

g. Arming arrangements.

h. Security arrangements within the public area, including arrangements for the security of VIP and Service enclosures, buildings, sensitive or similar installations, patrolling, both prior to, during and after the event.

i. Security arrangements within the non-public area, to include arrangements for the security of buildings and installations, patrols etc.

j. Arrangements to ensure the security of materiel and equipment.

k. Contingency plans for dealing with incidents and emergency situations, to include immediate reaction drills, command and control arrangements, allocation of resources, media arrangements and pre-determined public address broadcasts.

l. Measures to heighten security awareness.

Security within the Public Area of the Establishment

2. **Minimum security precautions.** The following minimum security measures are to be implemented within the public area of the establishment:

a. **Public entrances.** Wherever possible, public access to the event is to be through dedicated entrances that afford direct access to the public areas of the establishment; the location and number of entrances being dictated by local circumstances and topography. If, due to geographical constraints, it is necessary to allow members of the public to access the Open Day through gates that would normally serve the non-public areas of the establishment, such as the establishment Main Gate, suitable physical barriers are to be erected along the access route to prevent members of the public gaining access to that part of the establishment that is not open to them. Under such circumstances, a new, temporary, access point serving the non-public area should be constructed at some convenient location. Consideration is to be given to the provision of facilities for the random searching of vehicles as a deterrence measure.

b. **Public car parks**. The siting of public car parks will be dictated by the layout of the establishment; however, public car parks are not to abut static equipment displays or public buildings so as to avoid collateral damage in the event of an explosion. Additionally, consideration is to be given to:

(1) The provision of 'fire lanes' within the car park to allow easy access for emergency vehicles.

(2) The provision of a dedicated and secure parking area for VIP guests.

c. **Exhibitors and Traders.** Other than military participants or other official bodies of similar standing, traders and exhibitors are not to be allowed access to the non-public areas of the establishment. They should access the show site through either the public entrance gates or through a separate, dedicated, entrance provided for that purpose. Additionally:

(1) Trade stands and displays are to be sited far enough away from static equipment to avoid collateral damage in the event of an explosion.

(2) All trade and exhibition stands are to display a locally produced certificate of authority to trade or display.

(3) A member of the security staff is to brief all traders and exhibitors upon arrival about basic security precautions to be observed on the establishment. In particular, the briefing should include:

(a) Actions to take during an incident or emergency.

(b) The need regularly to check the stall or exhibit, including the immediate surrounds, for any unidentified items that may have been left or secreted.

(c) The need to report any suspicious incidents or activities.

(4) Other than military personnel who have made appropriate arrangements for accommodation, exhibitors and traders are not to be permitted to remain on the establishment overnight prior to, or immediately following, the event.

(5) A written security brief that covers the above points is to be prepared and issued to the person in charge of each stand or exhibit.

d. **Security patrols.** Routine, high visibility, security patrols are to be mounted continuously within the public area. The number of personnel employed upon patrol duties will be dictated by the physical layout of the area and the anticipated size of the crowd.

e. **VIP and dedicated Service enclosures.** Facilities provided for VIPs and enclosures set aside solely for use by Service personnel and their families, such as mess enclosures, are to be the subject of specific security precautions, to include:

(1) Control of access to the area and the identification of personnel present. Consideration should be given to the introduction of an identification 'badge' system.

(2) Regular checks of the enclosures for suspicious items.

(3) The briefing of staff employed therein on the need for increased vigilance within the area.

f. **Building security.** Additional security measures are to be taken to safeguard buildings and their occupants, including:

(1) **Buildings that are open to the public.**

(a) Each building that is open to the general public is to have a dedicated security guard force, members of which are to continuously patrol the building, both internally and externally, to ensure that items have not been left or secreted that could contain an explosive device. The size of the guard force will be dictated by the size of the building and the anticipated numbers of personnel present.

(b) The building is to be thoroughly searched and checked, both internally and externally, once the public have departed to ensure that:

i No objects have been left that could contain an explosive device.

ii No fire hazard exists.

iii It is properly secured.

(2) Buildings that are in use but not open to the public.

(a) Each building is to have an appointed building monitor, who is to remain in the building throughout the time that the public are present on the establishment, and who is to conduct regular security checks of the building, both internally and externally, to ensure that only authorized personnel are present and no items have been left or secreted that could contain an explosive device.

(b) Access points are to be reduced to a minimum, and strict control of entry is to be enforced.

(c) The building is to be thoroughly searched and checked, both internally and externally, once the public have departed from the establishment to ensure that:

i No objects have been left that could contain an explosive device.

ii No fire hazard exists.

iii It is properly secured.

(3) **Buildings that are not in use.**

(a) Each building is to be checked and properly secured before the public are granted access to the establishment.

(b) Security patrols are to confirm the security of the building at regular intervals throughout the time that the public are present in the establishment.

(c) The building is to be thoroughly searched and checked, both internally and externally, once the public have departed from the establishment to ensure that:

i No objects have been left that could contain an explosive device.

ii No fire hazard exists.

iii It is properly secured.

Security within the Non-Public Area of the Establishment

3. **Security Alert State.** The notified BIKINI or KEENWIND Alert State prevailing at the time of the open day is to be maintained throughout the non-public area of the establishment. However, plans are to be formulated to rapidly implement increased security measures in response to an increase in the local Alert State, should this prove to be necessary.

4. **Minimum security precautions.** The following minimum security measures are to be implemented within the non-public area of the establishment:

a. **Alert State measures.** Routine Alert State security measures are to be strictly enforced. In particular:

(1) Objects that could be used to conceal an explosive device are to be moved at least 25 metres from all buildings.

(2) The 25 metre parking rule is to be adhered to strictly.

b. **Control of entry.** Strict vehicular and pedestrian control of entry is to be exercised to the non-public area. Random searches of vehicles are to continue. Where there is no other recourse but to allow members of the public to access the Open Day through gates that would normally serve those areas of the establishment that are not open to the public, such as the establishment Main Gate, it may be necessary to establish a secondary, temporary, control of entry point at the boundary between the public and non-public areas.

b. **Barriers.** Where suitable permanent structures do not already exist, temporary, robust, physical barriers are to be erected along all boundaries between the public and non public areas of the establishment. The hire of 'Readyfence' or some other similar temporary fencing system should be considered. Because of the risk of accidental injury, the use of barbed fencing should be avoided in those areas that abut public access routes or areas.

c. **Security patrols.** Sufficient security patrols are to be mounted within the non-public area to detect and apprehend any unauthorized person, or member of the general public who may have gained deliberate or inadvertent access to the area. Patrols are to pay particular attention to:

(1) Domestic facilities including clubs, accommodation blocks and messes.

(2) Establishment boundaries, particularly where physical defences are inadequate to prevent members of the public gaining access.

d. **Identification.** All establishment personnel, including dependants contractors, honorary Mess members etc, who have a bonafide reason for being within the non-public area, are to carry some form of authorized identification. Consideration should be given to adopting some form of temporary 'badge' system for ease of identification.

e. **Access to the non-public area.** Access points linking the public and non-public areas are to be manned by Service personnel who are to exercise strict control of entry, including rigorous identity checks of any person seeking entry to the non-public areas of the establishment.

f. **Sensitive installations.** Consideration is to be given to providing sensitive installations, including fuel and explosive storage areas, with a dedicated guard force who are to be located within or around those installations whilst the public are present on the establishment.

g. **Building security.** Additional security measures to be taken to safeguard buildings and their occupants are:

(1) Securing buildings that are not in continuous use.

(2) Exercising strict control of entry on all buildings that are in use.

(3) Thoroughly searching and checking each building, both internally and externally, once the public have departed from the establishment to ensure that no object has been left or secreted that could contain an explosive device.

APPENDIX 5 TO ANNEX I TO SECTION IV TO CHAPTER 7

OFF SITE EVENTS

Off Site Events (Excluding PMEs) - Physical Security General

1. The terrorist threat increases the risk to any MOD activity held off MOD property, particularly where members of the Armed Forces are involved, and when any members of the public have prior knowledge of the event. If the terrorist threat to an identifiable MOD organized or sponsored Off Site Event (OSE) is assessed at SIGNIFICANT (Level 3) or higher, whenever possible the event should be held on MOD premises.

Events Covered by this Instruction

2. Examples of OSEs covered by this instruction include conferences, seminars, lectures, dinners or other social gatherings arranged by MOD for MOD Service personnel or civilian employees, where either the public is excluded or only very limited numbers are invited individually. Public Military Events (PMEs) are not covered by this instruction nor are the existing rules for PMEs altered in any way. (PMEs are events to which the public has both access and prior knowledge. Security instructions for PMEs are contained in paragraphs 07448 - 07469).

Action to be taken

3. At the initial planning stages of an OSE, prior to the booking of a venue, an Event Security Officer (ESO) is to be appointed. The ESO is to inform the Establishment Security Officer (ESyO) of the proposed OSE. If the ESyO requires additional advice, especially where the event may fall under the definition of a PME, this is to be sought through the chain of command or from the appropriate PSyA or Command security staff. ESyOs are to maintain lists of all current OSEs within their locality, keeping the local police informed as appropriate. In addition, ESyOs for all OSEs sponsored by the Royal Navy are to contact their local RN Area Security Team.

4. Maintaining the anonymity of the MOD connection is the most important factor in OSE planning; from the time of the initial booking or enquiry, to the conclusion of the event. When making the booking the venue should be told not to record or publicise the MOD connection (for example on notice boards or directional signs). Where possible the booking should be with an address that does not reveal any MOD or military connection. All those attending the function are to be forewarned to use the event's pseudonym when contacting the chosen venue. Additionally, event organizers are to note the following:

a. Repeated and regular use of the same venues should be avoided.

b. Loose talk in public areas of the venue that may identify the participants with the MOD should be avoided.

c. Sponsors, organizers and participants are to be reminded of the current threat assessment and of their individual personal security responsibilities.

d. Normally, the participants, including guest lecturers or presenters, should not wear Service uniform.

e. The ESO, assisted by suitable personnel, should search the venue, inconspicuously if possible, before the event. Subsequent admission should be controlled until the event is completed.

f. Participants are to be reminded to be alert and vigilant for suspicious persons, packages and vehicles.

g. Invitations and identities of attendees are to be checked against a master list.

h. At social gatherings, such as in hotel bars or restaurants, individual(s), who should not drink alcohol, are to be detailed to remain on watch both inside and, if appropriate, outside the area concerned. (SHARKWATCH).

i. Service transport is not to be used to travel to and from the venue unless it has been 'civilianized' and service drivers should not wear uniform. Security of vehicles will normally remain the responsibility of the owner or driver.

ANNEX J TO SECTION IV TO CHAPTER 7

GUIDANCE ON COUNTER TERRORIST SEARCH AWARENESS SECURITY MEASURES (CTSASM)

Individual CTSASM

1. **General.** Individuals can play a vital part in ensuring their own safety, and that of others in their immediate vicinity, by being alert and punctilious in their application of CTSASM.

2. **Measures.** Individual CTSASM include:

a. **Knowledge of surroundings.** A sound knowledge of their local surroundings is essential if individuals are to notice that which is out of place. It is the responsibility of every individual to familiarize themselves with their work area, living accommodation and their private transport so they can complete quick and effective searches.

b. **Tidiness.** Individuals should be encouraged to keep their work and living accommodation areas tidy. This will minimize the scope for hiding devices and aid both the occupant and deployed search teams to check more quickly a building and its surrounds.

c. **Routine checks.** Checks and searches of an individual's environment are essential and must be carried out as a matter of routine. Key times for such searches include:

(1) Before getting into a vehicle that has been left unattended.

(2) Returning to accommodation that has been unoccupied.

(3) Entering an unguarded place of work that has been left unoccupied.

d. **Observation.** Individuals need to be alert to observe unusual and suspicious occurrences.

3. **Unit action.** Individuals should be briefed regularly on CTSASM and checks carried out within units to ensure that preventative measures, including tidiness and routine checks, are being applied.

Establishment CTSASM

4. CTSASM for establishments are both preventative and protective. The following measures applied at unit level by search aware personnel should greatly increase the unit's level of security:

a. **Verification.** Effective measures to verify the authority for people and vehicles to be within an establishment perimeter will reduce the search burden.

b. **Surveillance.** Consideration should be given to countering terrorist surveillance by:

(1) Identifying potential observation points and lines of sight into and within the location.

(2) Use of screening.

c. **Checks.** Repetitive routines must be monitored, set patterns varied and checks conducted in a random and unpredictable manner. Checks should include:

(1) **Routine checks.** The reason for and thoroughness of routine checks must be emphasized. For the most part, they are dull and boring and are only really effective if those involved know what they are looking for and why.

(2) **Random checks.** Random checks are effective but disruptive. However, very few are needed to create uncertainty in the mind of a would be attacker. Random checks should be carried out as follows:

(a) **Vehicles.** Random vehicle checks in public view have an enhanced deterrent effect.

(b) **Visitors.** A thorough search of a small sample of visitors' baggage provides a good degree of security with the minimum disruption.

d. **Specialist areas.** Complex buildings, vehicles and equipment require special arrangements to ensure that those familiar with them are available to carry out searches as necessary.

e. **Tidiness.** Searching is made more difficult by the presence of rubbish and other waste items that could hide a bomb. Measures to ensure that rubbish areas are kept tidy, secure and regularly emptied should be put in place.

f. **Accommodation block fittings.** The number of fittings such as bins, traffic cones and fire extinguishers, that could hide bombs, must be kept to a minimum.

g. **Sealing.** Where possible, those areas and spaces that might be used to hide bombs should be searched and sealed so that unauthorized entry can be more readily detected.

h. **Horizontal surfaces.** Horizontal surfaces, such as flat roofs, are suitable platforms for bombs and can provide cover from view. Such areas must be searched more regularly than most.

Guidance on the Formulation of a Search Plan

5. **Stage One.** Conduct a vulnerability assessment as follows:

a. Identify those buildings that are most vulnerable and which terrorist might wish to attack, i.e. living accommodation, messes, guardroom, NAAFI.

b. Buildings should be graded as follows:

(1) High Risk (RED) i.e. living accommodation.

(2) Medium Risk (AMBER) i.e. working areas and offices.

(3) Low Risk (GREEN) i.e. buildings that are rarely occupied such as garages and stores.

6. **Stage Two.** Use this colour system to plot the vulnerability assessment onto a plan of the establishment. Colour coding will provide priorities for search, i.e. RED area first.

7. **Stage Three.** Sub-divide the establishment into sectors providing the following:

a. Set areas of search responsibility with well defined boundaries.

b. These areas should be plotted onto search sector cards which are issued to each search team by the search organizer. Each card should include any relevant information for that given area of responsibility e.g. simplex lock combinations. (Keep cards under lock and key when not in use).

Conduct of Search

8. **Stage One.** The search organizer assembles search team leaders and allocates search tasks and sector cards. A record should be kept of potential team leaders who should ideally have had previous search experience. It is recommended that search team leaders with a detailed knowledge of particular areas should be given those to search.

9. **Stage Two.** Teams are assembled and briefed by their team leaders. Each team should consist of up to 10 search aware personnel drawn from whoever is available within the unit.

10. **Stage Three.** The actual search should be conducted as follows:

a. **Buildings.**

(1) Carry out an external search of walls, foliage, the roof and refuse areas. Do not forget to search for disturbed ground where an IED may have been buried in close proximity to an external wall.

(2) Search those internal areas that are easily accessible such as ablutions, rest rooms, stairwells and corridors.

(3) Search those internal areas that are not easily accessible such as accommodation rooms, false ceilings and attics.

(4) Search starting on the ground floor and clearing each floor before moving up.

(5) A room should be searched as follows:

(a) A pair of searchers start at the entrance. One works clockwise and the other anti-clockwise.

(b) They each carry out sweeps at floor, mid and ceiling level. Be sure to search the middle of the room including any furniture.

(c) Each searcher starts and finishes at the door.

b. **Co-ordination.** As buildings and or sector searches are completed the team leader should report back to the search organizer. The team leader should be sited at a suitable control centre.

Search and Seal Option

11. To save time and effort, consideration should be given to the use of "Tamper Evident Seals". Buildings, rooms, containers or any other equipment that lends itself to sealing that are rarely used or vacated at weekends or at night should be sealed on exit, removing the need to search them. Seals are then easily checked for sign of forced entry. If used, seals should be applied to all entry points, checked regularly and recorded in a register. Seals should be regarded as an aid to searching and not a replacement.

Search Equipment

12. Search equipment should be easily accessible and possibly held in the guardroom and should include:

a. Torches.

b. Telescopic mirrors.

c. Ladders.

d. Screwdrivers.

e. Sector cards.

f. Tamper evident seals.

g. Radios.

h. Safety harness.

i. Periscopes, endoscopes.

j. Rolling boards for under vehicle search.

Search Advice

13. Search advice is available on request from the following sources. If in doubt as to who to consult an approach should be made initially to the FSC at the appropriate HQ.

a. The FSC on the 2SL/CINCNAVHOME staff.

b. P&SS FSA (through P&SS Regions).

c. The STIRC at NSC Carver Barracks.

d. Police Search Advisers within the Home Department police and MDP.

This page intentionally left blank

SECTION V TO CHAPTER 7

PERSONAL COUNTER TERRORIST SECURITY MEASURES

General

07501. Certain terrorist organizations have shown that they may consider personnel with MOD connections to be "legitimate targets". During a terrorist campaign, therefore, all personnel are at risk from attack. An attack could materialise at any time or place and personnel need to remain vigilant even when at home or travelling.

07502. Within GB, the standard graded threat levels are also used to indicate the level of threat to an individual. The definitions of the threat levels have been previously described in Section I paragraph 07107.

07503. If it is considered than an individual, of whatever rank, is at a higher risk of terrorist attack then a special threat assessment should be sought from D Def Sy through the appropriate PSyAs and Command security staff. If that assessment places the individual at threat level 3 or above, then special protective measures will be implemented - see also paragraphs 07509 - 07515.

Terrorist Targeting

07504. Terrorist organizations use open source material to obtain information for use in targeting personnel. A wide variety of information sources are used for this purpose including the media and publications such as telephone directories, electoral rolls, "Who's Who", the Service Lists and Service journals.

07505. In addition, terrorists can be expected to conduct general observations and target reconnaissance of personnel or target areas such as Service families accommodation, places of entertainment used by personnel and routes used to travel to and from work.

07506. The greatest contribution to personal safety can be made by:

a. Alertness and vigilance.

b. Avoidance of routine patterns of activity.

c. Adoption of sensible and practical personal security drills.

d. Remaining, as far as possible, anonymous.

07507. Guidance to counter targeting of individuals by terrorists are detailed in the following Annexes. Not all the advice needs to be followed by everyone all of the time. The HOE has a duty of care to ensure that personnel should adopt those measures that they

see as appropriate to their circumstances bearing in mind the level of threat that pertains at the time.

a. Security at home - Annex A.

b. Security when travelling - Annex B.

c. Security at places of entertainment - Annex C.

d. Dealing with the media - Annex D.

Anonymity

07508. When a serious terrorist threat has been identified, personnel should be alert to the dangers of unnecessarily identifying themselves as being members of the MOD or Armed Forces. The following list, whilst not exhaustive, is intended as a reference guide to those areas where identification with the Services could be avoided:

a. **General.**

(1) Avoid wearing uniform or using military equipment in public.

(2) When out of uniform avoid wearing MOD or Service related T-shirts or sweatshirts in public.

(3) Avoid disclosing MOD or Service connections to strangers.

(4) Do not wear establishment passes outside your place of work. Colleagues wearing passes in public should be warned of the risks that they are incurring.

b. **House.** Do not include Service details in documents and correspondence relating to:

(1) Council Tax.

(2) Electricity, gas, oil and water.

(3) TV licence.

(4) Telephone bill.

(5) BT directories. (Consider an ex-directory telephone number or requesting BT to omit a directory entry but to make details available through directory enquiries. In any event, an entry giving rank should be avoided).

(6) Insurance - buildings and contents.

(7) Appliance warranties and guarantees.

c. **Vehicle.** Do not include Service details in:

(1) Registration book.

(2) Insurance certificate (where avoidable).

(3) Driving licence.

(4) Vehicle servicing log book.

d. **Bank and Building Society.** Do not include Service details in:

(1) Cheque books.

(2) Cheque guarantee and credit cards.

(3) Building Society account books.

e. **Personal.** Do not include Service details in:

(1) Warranty and guarantee certificates.

(2) Bus and rail passes (unless HM Forces Railcard).

(3) Market research questionnaires.

(4) Concession and discount application forms.

(5) Membership cards for clubs, motoring organizations etc.

f. **Electoral Registration**. The Representation of the People Act 2000 came into effect on 16 Feb 01 and introduced a number of changes to electoral registration procedures. Electoral Registration Officers are now required to make copies of their electoral registers available for sale. Two versions of the electoral register will be produced. The full version will be used for electoral and law enforcement purposes, and will be available for banks and other credit institutions to check identity in credit applications. It will be an offence to use the full version of the register for any other purpose. An expurgated version will be available for general sale. Individual electors, including Service personnel, will be given the option of deciding whether all of the details they provide for registration purposes should be included in the commercially available register. They are also able to opt out of having their names, or any other details, included on the register that will be made available for commercial use

g. **Absent Voting.** The rules for those individuals that elect to vote by means of a Service declaration remain unchanged. Those overseas can only vote by proxy, while those physically in the UK but who are unable to vote in person, may vote by either post or proxy. Those individuals that choose to register on a local electoral register, and who are not registered as Service voters through a Service declaration, will be able to vote either by post or proxy if they are overseas or away

from home during an election or are disabled. All personnel will need to contact their local Electoral Registration Office directly if they wish to register under these arrangements.

h. **Council Tax.** A legal right exists in the Council Tax legislation for individuals who believe themselves to be at risk of violence to request anonymous registration with local authorities. MOD has been informed that local Council Tax registration authorities are likely to treat applications from Service personnel for anonymous registration favourably. The following advice is therefore given to establishments, units and individuals in GB:

(1) Lists of those living in accommodation blocks should be submitted by establishments to the local authority requesting anonymous registration.

(2) Those living in Service families and private accommodation should apply for anonymous registration individually.

i. **Schools.** Parents of children at boarding school should warn the staff of the school of the need, especially in periods of high threat, to exercise careful control over information that may identify Service parents.

j. **Release of information to commercial companies.** Before voluntarily divulging personal information to commercial companies, individuals should ensure that the potential recipient has a genuine need to know the information. Wherever possible, avoid the use of MOD or Service details. When completing forms requiring to know an individual's occupation the term "Government Service" should be used whenever possible. However, where an accurate description of employment, e.g. for insurance and mortgage purposes, is required this may not be possible. In such circumstances it may be necessary to reveal a Service connection to ensure that the policy's validity cannot be questioned.

k. If Service details have to be divulged the following should be applied:

(1) Only supply the minimum of information and ask permission before providing personal details of employers or superior officers for reference purposes.

(2) Ask the commercial organization to provide a written undertaking to the effect that Service details will be omitted from any correspondence, the information will be handled in the strictest confidence, not recorded on an IT database or disclosed to third parties.

l. **Mailing lists.** If personnel find their names on mailing lists, these can be removed by applying to the Mailing Preference Service, 1 Leeward House, Plantation Wharf, London, SW11 3TY or FREEPOST 22 London, W1E 7EZ. This firm will normally assist where the individual is on a list maintained by one of the firm's subscribers. There is, however, no guarantee that any name can be removed from all lists world-wide.

Protection of High Threat Personnel (HTP)

07509. In addition to the requirement to protect all Service personnel from the general threat of terrorism, it is sometimes necessary to provide enhanced protection for particular individuals, known as High Threat Personnel (HTP), who are assessed to be at higher threat of attack because of:

a. The nature of their service in relation to counter terrorist operations;

or

b. the status and high profile of their appointment;

or

c. other factors serving terrorist propaganda objectives.

Action in GB

07510. The Security Service informs D Def Sy and provides a threat assessment if intelligence is received that a particular individual is targeted by terrorists. In addition, advised by the CEAG, D Def Sy nominates a small number of personnel who match interdepartmental criteria developed from the factors at sub-paragraphs 07509 a to c above, for assessment by the Security Service. Vulnerability and risk are taken into account. Those assessed to be at or above **Significant** threat (level 3) (see paragraph 07107 for definition) are categorized High Threat Personnel (HTP) and certain essential protective security measures (PSM) are authorized for them. These are in line with interdepartmental standards and are additional to or subsume any measures provided under the terms of Chapter 5. If armed protection is justified it is provided by the appropriate Home Department Police Force (HDPF). A list of HTP is published periodically by D Def Sy.

Action in NI and Overseas

07511. In NI and overseas the decision on whether and to what extent enhanced PSM should be provided for an individual at higher threat is to be made by the commander concerned, based on a threat assessment and recommendations provided by the security staff. Any host nation provision should be taken into account; whether this includes armed protection depends on relevant inter-governmental agreements. If appropriate, security staffs should seek a Security Service assessment of the threat to individuals overseas through MOD D Def Sy. Such requests should attach a report assessing the vulnerability of the subject. Where personnel assessed below threat level 2 are, nevertheless, considered by PSyAs and Command security staff to be at exceptionally high risk, they may decide to protect them as though they were HTP at that threat level. Names of personnel in this category should be notified to D Def Sy as they arise.

Protective Security Measures

07512. These should take into account the modus operandi of the terrorist group(s) concerned and might include:

a. The appointment of a single point of contact (POC) responsible for all contingent security advice and assistance to the HTP, his family and staff.

b. Personal security drills at home, at work, during visits, while travelling, during recreation and at official and private social events.

c. The security vetting of household staff.

d. Physical protective security measures at the home and place of work of the HTP.

e. Close protection (CP) (see paragraph 07523 below).

f. Provision of an armoured staff car (CSAP).

g. Provision of a reaction force.

h. Protection of information to avoid publication, whether official, private or in the media of the individual's location, movements and general activities.

Close Protection

07513. Close Protection (CP) is the armed protection by Service police or other specially trained personnel of an individual (the "principal") against unconventional, direct, harmful attack at close quarters. Its sole aim is to protect the principal. In conventional military operations or where enemy Special Forces (SF) may be deployed, CP is a matter for the operations staff advised by the intelligence staff. The intelligence staff provide assessments of the threat upon which decisions are made. Armed protection of HTP in mainland GB is the exclusive responsibility of HDPF. Where there is a terrorist threat or the risk of attack by other violent extremists in NI or overseas the security staff should advise whether CP is appropriate. CP will usually be appropriate for HTP assessed to be at threat levels 1 or 2.

Armoured Staff Cars

07514. The provision of an armoured staff car, Car Saloon Armoured Protected (CSAP), to protect against terrorist attack is justified where an HTP at higher threat (levels 1 or 2) is required to travel by road in high risk conditions. In GB the HDPF personal protection officers (PPOs) of HTP at threat levels 1 or 2 will decide whether an MOD provisioned CSAP is appropriate for a particular journey. In NI and overseas, where CP is provided by Service police or the host nation, a CSAP will be required for those high risk journeys where an operational road vehicle or helicopter is unavailable or its use is impracticable or inappropriate. Alternative methods of risk reduction, such as the use of a hired indigenous vehicle to achieve anonymity, should also be considered.

The Protection Plan

07515. The protection plan must make it clear that the greatest contribution to an individual's personal safety is achieved by strict observance of four key factors:

a. **Alertness**. HTP and their families and staff should be inquisitive and alert at all times for the many sources of danger. The security staff, security unit POC, the HTP and his personal staff should examine the individual's security arrangements from the terrorist viewpoint to see whether they can detect any weaknesses.

b. **Avoidance of routine patterns of activity**. Regular patterns of activity should be avoided; where this is unavoidable those concerned should be fully aware of the risks and take appropriate precautions.

c. **Adoption of practical security drills.** The adoption of simple, common sense security drills make an individual a harder target.

d. **Anonymity.** No matter how inconvenient, outside Service establishments, particularly where an HTP lives, shops or takes recreation, the HTP should make it as difficult as possible to be identified with the Services.

Home Security

07516. Guidance on personal security at home is given at Annex A to this Section.

Survival in Hostage Situations

07517. Guidance on survival in hostage situations is given at Annex E to this Section.

This page intentionally left blank

ANNEX A TO SECTION V TO CHAPTER 7

GUIDANCE ON PERSONAL SECURITY AT HOME

General

1. This guidance is designed for personnel at higher threat (HTP) but all should draw on it as necessary to suit their own particular circumstances. This Annex is designed to be read by the individuals concerned.

The Key to Successful Protection

2. The most important thing to remember is always to be on the alert for terrorist sources of danger, particularly when you are most vulnerable, such as when leaving or entering your home or place of work. You should avoid creating a regular pattern of behaviour. The adoption of the simple personal security drills set out in this annex will make you a less likely target for terrorist attack.

Anonymity

3. You should avoid giving information about where you are going and what you are doing. You should aim to achieve anonymity outside Service establishments, particularly where you live, shop, or take recreation. In particular, you should:

a. Ensure that military stores such as MFO boxes and items of uniform are not left outside your house or in your private vehicle where they can be seen by strangers.

b. As far as possible, avoid wearing visible items of uniform when travelling to and from work.

c. Whenever possible, avoid being collected at home by non-civilianized Service vehicles or drivers in uniform.

d. Whenever possible, avoid disclosing your Service connection to professional and commercial organizations or utilities who may record it in their data bases and issue documents, such as credit cards and cheque books to you, or correspond with you. Do not authorize the publication of your rank or Service in telephone directories, the electoral roll and other easily accessible records. It is advisable to have your telephone number ex-directory.

e. Use a forwarding rather than a private or official address in such publications as 'Who's Who', or in open registers published by clubs and societies.

f. Arrange for your private and personal mail to be addressed to your office and not to your private address. Ask anyone who may correspond with you to omit your rank from any mail sent to your private address.

Locks and Keys

4. Secure locks and good key control are essential security aids. Cheap locks are easily picked and secure locks are only effective if the keys to them are properly protected as follows:

a. Keep a strict check on your house keys.

b. Do not allow duplicate keys to be made without your permission.

c. If a key is lost in suspicious circumstances, report the fact and have a new lock fitted.

d. Working keys should never carry any form of written identification. If you need to identify keys, a system of colour coding could be used.

e. Never leave keys under the mat or in other obvious hiding places.

f. Spare keys should be held in a central location not accessible to visitors.

Doors and Windows

5. You are particularly vulnerable when answering the door. Do not answer the door automatically in response to a knock or bell. Check who is there by observing through an adjacent window, by using an entryphone, if installed, or by using a door viewer if fitted. You should note the following points:

a. If suspicious of any caller do not open the door.

b. When answering the door, do not put on the hall light. An external light in the vicinity of the door should be kept burning during the hours of darkness, see paragraph 7.

c. If you have glass panes in the door, prevent observation by, for example, fitting a thick curtain.

d. Keep access windows locked.

e. After dark, keep curtains or blinds closed. Remember to draw curtains before switching on lights and switch off lights before drawing back curtains in order to avoid being silhouetted at windows.

f. Make a safety check each night before retiring to ensure that all doors and windows are properly closed and locked.

g. Have a security chain fitted to the door.

Garden, Garage and Outbuildings

6. Doors and windows of garages and outbuildings should be kept locked, except for specific access. The following additional action should be taken:

a. Consider locking drive gates with a security lock to prevent vehicle entry.

b. Doors and windows of garages and outbuildings should always be checked for signs of unauthorized access before entering.

c. Bushes, trees and undergrowth providing cover, especially close to the house, footpaths or driveways, should be removed or trimmed to make it more difficult for an intruder to operate or to conceal an explosive device.

d. If possible refuse bins should be kept in an enclosed area.

e. Do not handle anything suspicious - call the police.

Lighting

7. At least one strong light should be kept burning in the area of the front door during hours of darkness, so that you do not signal your approach to the door by turning on a light. Remember:

a. If you go out at night prepare for your return before leaving. Turn on any outside approach lights and lights in the garage, leave a light burning in the house in a regularly used room - not just the hall light. Consider using a light plugged into a time switch that will simulate activity within the house; do not overlook the need to vary timing and position.

b. Always have some reserve lighting to hand such as torches, candles or lamps.

Telephone

7. Site your telephone in such a position that you cannot be observed through windows or doors when using it. Consider having an extension in the bedroom. Also:

a. If your telephone is out of order, report it immediately and be especially vigilant until it has been repaired.

b. Keep a list of emergency numbers near the telephone.

c. Other members of the household, especially staff, should exercise discretion when answering the telephone. No information should be given concerning your whereabouts, movements or future appointments, or those of your friends and colleagues. The caller's name, address and telephone number should be taken so that you can return the call.

d. Telephones fitted with BT caller display and call return services can identify the number you call from. Consider having your telephone blocked from this service. Alternatively, by dialling **141** before the number called your number will be protected. This service may be useful for the tracing of anonymous or threatening calls - by dialling **1471** immediately after the call is received.

Visitors, House Staff and Tradesmen

9. All visitors should be positively identified before being allowed to enter, in particular:

a. Arrange fixed times for workmen to call. Check their identity and never leave them alone in the house. If they are unexpected, call their works office.

b. Friends and relatives should be asked to inform you of intended visits whenever possible, particularly if they plan to arrive at an unusual time.

c. Very late callers should be treated with particular suspicion.

d. Check newly engaged staff. If additional staff are engaged for a function they should be vouched for and identified by a responsible person.

e. **Deliveries by tradesmen**

(1) Do not accept parcels that have not been ordered.

(2) Discourage the leaving of parcels or bags on window sills or at the door.

(3) Deliveries should be checked carefully before accepting them and the person making the delivery detained until this has been done.

(4) Be suspicious of any change of postman, milkman or other regular delivery men.

(5) Stop deliveries of milk, papers, etc, when going away.

(6) Particular care is needed when removing routine deliveries such as milk or newspapers; first, you may expose yourself in a routine manner and secondly, deliveries can easily have explosive devices attached that may be difficult to see, particularly on dark mornings.

Mail

10. Familiarize yourself with action to be taken on receipt of a letter or package that might contain an explosive device.

11. Guidance on the advice you should give private correspondents addressing mail to you is given in paragraph 3.

Alarms

12. Consider fitting a 'panic alarm' bell to the outside of the house with switches upstairs and down. Consider an alarm to a neighbour's house.

Private Social Activities

13. Invite only guests who are known to be reliable and do not present a security risk. Care must be taken in the issue of invitations to large functions.

14. Vary your times as much as possible for sporting activities, e.g. visits to a golf club, tennis courts, etc. Do not regularly go walking alone in the country, or go on lone fishing trips, etc.

Personal Security of Children

15. Ensure that children's rooms are not readily accessible from outside the house.

16. Instruct children never to admit strangers to the house. As soon as they are able to learn, teach them when and how to alert police or neighbours.

17. Instruct children attending school always to:

a. Travel in groups or at least pairs.

b. Use well frequented thoroughfares.

c. Avoid play-areas outside the school.

d. Refuse gifts or approaches from strangers.

e. Report attempts of an approach immediately to the nearest responsible adult, and tell you as soon as possible.

f. Tell you at all times where and with whom they will be, when away from the house.

g. Never discuss what you do and to tell you if they are ever questioned about you by anyone.

18. Encourage your children to report suspicious incidents to you.

19. Young children should be accompanied to and from bus stops, where necessary. Also:

a. Do not allow pre-school children to wander from the house or to play in areas where they cannot be supervised.

b. Discourage children from answering the door, especially during hours of darkness.

c. Do not allow younger members of the family to collect or open your mail.

d. Young children should be discouraged from answering the telephone, as they may unintentionally give out information detrimental to your safety.

e. Employ only mature, responsible baby-sitters in whom you have complete trust. Ensure that they are well acquainted with procedures for opening the door and answering the telephone and make sure that they know where you can be reached, and where to find emergency telephone numbers.

f. If a child is attending school, arrange with the school authorities to contact you before releasing the child to the custody of anyone you have not previously nominated. If the school is a day school, arrange for the child to be accompanied on each journey by a responsible adult or by other children.

Absence

20. If you leave your residence for a period of days, ensure it is locked and secured. Arrange for visits to be made by the police and neighbours. On return be suspicious. Do not push excessively against a door that normally opens easily.

ANNEX B TO SECTION V TO CHAPTER 7

GUIDANCE ON PERSONAL SECURITY WHEN TRAVELLING

1. The following guidance is intended to offer general advice to personnel when travelling. Personnel should adopt measures as appropriate to their circumstances, the assessed level of terrorist threat and Alert State.

2. Never make a journey or keep an appointment without informing family or colleagues of the following:

   a. Destination.

   b. Person to be visited.

   c. Method of travel.

   d. Expected time of arrival.

   e. Expected time of return.

3. Avoid travelling in uniform including to and from work. If the wearing of uniform cannot be avoided, it is recommended that a civilian jacket or coat is worn to cover the uniform when in the vehicle (mixed dress in public is not encouraged). **NEVER** hitch hike in uniform.

4. Never allow yourself to be driven by anyone who is not known to you other than on accredited public transport.

5. Be alert for anything unusual or out of place at the beginning and the end of the journey.

6. Check the driveway and road before leaving home.

7. Be alert to suspicious or unaccountable conduct by persons in the vicinity of the home or place of work. Be particularly aware of manned vehicles, people tinkering with vehicles and innocent seeming workmen from service industries.

8. Restaurant, hotel and travel reservations should be made without reference to rank, title or, where avoidable the Services.

9. Avoid travelling, working or staying overnight in conditions that involve isolation from persons able to give or summon assistance. Always have to hand or in mind a ready means of communication or of otherwise attracting attention.

10. **By private vehicle.**

a. **Counter measures to the UVIED threat**.

(1) Know your vehicle thoroughly, when searching for an IED you must know what ***should be*** attached, inside or underneath.

(2) Keep your vehicle in good condition and regularly serviced.

(3) Never leave your vehicle unlocked. Remember to secure all the doors, sunroof, bonnet and boot. Use the alarm or immobiliser if fitted.

(4) On returning to your vehicle, do not take it for granted that it is as safe as when you left it.

(5) Secure bonnet locks and lockable petrol caps should be fitted and used whenever possible.

(6) Never leave your baggage unattended outside the vehicle.

(7) Never carry other people's baggage or packages unless you have personally checked the contents.

(8) Do not display Service badges or stickers or leave military clothing or equipment visible in your vehicle. Vehicle passes should be concealed from view when outside MOD establishments.

(9) Carry a torch with you to check your vehicle after dark. Do not leave the torch in the vehicle.

(10) Switch off the courtesy light inside the vehicle to avoid illumination when getting in and out.

(11) Always try to park the vehicle in a lockable garage at home and at work. If no garage is available, leave it in a supervised car park or where the general public can see it.

b. **Searching.** Searching should be conducted routinely if your vehicle is used and parked in an area that is associated with the presence of Service personnel. You should exercise your judgement as to whether you should carry out a search of your vehicle if it has been left in other areas. Keep in mind the possibility of a terrorist being able to predict where the vehicle would be parked or being able to identify it as belonging to Service personnel. Remember that the very act of searching could draw attention to you and your vehicle. Care should be taken to ensure that the vehicle is not moved while conducting a vehicle search. Searching should be conducted by:

(1) First looking carefully around the outside of the vehicle.

(2) Looking at the doors, boot and bonnet for signs of tampering.

(3) Looking through the windows for any unidentified item.

(4) Checking around and behind each wheel and inside the wheel arches.

(5) Looking underneath the vehicle, using an angled mirror on a rod designed for the purpose if available, paying particular attention to the area of the drivers seat, the exhaust system, floor pan and behind and around the fuel tank.

(6) Unlocking the vehicle and checking the driver's area. Checking inside, including under seats, the glove compartment, under the bonnet and inside the boot area.

(7) If any signs of tampering are noted or anything suspicious is found such as unusual objects inside the vehicle or attached and out of place.

STOP

No attempt should be made to touch, start or move the vehicle. Keep all persons away from the vehicle. The police should be called immediately.

c. **On the move.**

(1) Ensure that windows are fully closed when the vehicle is parked and opened only enough for ventilation when you are driving.

(2) Look forward along the row of vehicles parked in the street for anything of a suspicious nature and through the driving mirror for following vehicles.

(3) Avoid narrow and lonely streets, keep to main routes.

(4) Conform to traffic flow but keep your distance from the vehicle in front.

(5) Try to avoid becoming hemmed in when held in traffic. At traffic lights leave enough room for manoeuvre. If possible, adjust speed when approaching traffic lights to avoid having to stop.

(6) If something suspicious appears to be taking place on the road ahead, stop and turn off before it is too late.

(7) If you suspect that you are being followed, try not to allow yourself to be overtaken or forced off the road. Take a known detour, and if still suspicious, stop at the nearest police station or Service establishment.

(8) Ensure that you have sufficient fuel to avoid stopping at unknown or isolated filling stations.

(9) Do not give lifts or open doors or windows to unknown persons.

(10) Beware of accident scenes in isolated areas; these may have been staged.

11. **Rail, sea, air and other means of travel**.

a. On a train, enter a compartment that is already occupied.

b. Baggage should be kept locked and within view wherever possible.

c. If you have had to surrender your baggage, make sure it is correctly identified on its return and that it has not been tampered with before opening it.

d. When travelling by ferry, be alert when walking on the deck at night.

e. At sea, try to obtain your own cabin and ensure that the door is kept locked.

f. Be cautious of sharing a taxi with unknown persons.

12. **Hotels**.

a. If you have to visit an area frequently, avoid using the same hotel on each visit.

b. Do not meet visitors in your room who are unknown or not vouched for. Meet them in a public room where others will be present.

13. **Use of Service issued baggage.** The use of Service issued baggage when travelling could identify the carrier as a Service person. Personnel are therefore advised:

a. Not to use items of Service issued baggage for leave and off-duty travel (except the 'civilianized' holdall).

b. To be aware of the security risk when travelling on posting or detachment on public transport with items of Service issued baggage.

APPENDIX 1 TO ANNEX B TO SECTION V TO CHAPTER 7

ADDITIONAL SECURITY PRECAUTIONS FOR STAFF CAR DRIVERS

1. The security precautions listed at Annex B are generally applicable to all drivers. The role of staff car drivers and their responsibility for passengers raise additional security considerations.

2. Units should examine the need to brief staff car drivers and potential passengers on the additional points outlined below:

a. **Picking up and setting down passengers.** This is a period of risk where habits may become dangerously routine. Both driver and passenger should agree, where applicable, to:

(1) Vary times.

(2) Vary points of arrival and departure.

(3) Vary general procedures in as many ways as possible.

b. **Waiting.** Staff car drivers may spend significant periods of time waiting. They should be aware that a more effective way of guarding a vehicle is to observe it from a sensible position outside the vehicle rather than by sitting in it.

c. **Actions on the move.** Drivers should be particularly vigilant and adopt the following procedures:

(1) Doors should always be locked and windows closed wherever possible.

(2) There must always be room to manoeuvre the vehicle. This means not getting boxed in by other vehicles or caught in traffic jams.

(3) If it is suspected that the vehicle is being followed, the following vehicle must not be allowed to overtake or to force the staff car off the road. Drivers should attempt to take a known detour. If there is still cause for suspicion, they should drive to and stop at the nearest police station or MOD establishment.

d. **Action if a staff car is directly threatened.** The following action should be taken if there is direct threat:

(1) Use horns, lights or any other means to attract attention.

(2) Use rapid acceleration or sudden braking to outwit the attacker(s).

ANNEX C TO SECTION V TO CHAPTER 7

SECURITY AT PLACES OF ENTERTAINMENT

1. In GB, places of entertainment (e.g. public houses, wine bars, restaurants and even theatres) have in the past been attractive targets for terrorist attack. The measures advised below should be adopted in places of entertainment as appropriate.

2. Be alert and vigilant for suspicious persons, packages and vehicles.

3. Avoid talking about matters that identify you as a member of the MOD or Armed Forces.

4. Do not wear uniform, unit ties, blazers with official crests, T-shirts or sweatshirts with MOD logos or any item of clothing that would identify you as a member of the MOD or Armed Forces.

5. At large group gatherings, an individual, who should not drink alcohol, should be appointed to remain on watch both inside and outside the place of entertainment; this is known as SHARKWATCH.

6. Do not make "bookings" using MOD or Service details.

7. Repeated and regular use of the same place of entertainment should be avoided.

8. Do not use Service or MOD transport to travel to and from the venue unless it has been civilianized.

9. Do not place anything in or on your vehicle that would identify you as a member of the MOD.

This page intentionally left blank

ANNEX D TO SECTION V TO CHAPTER 7

DEALING WITH THE MEDIA

1. **Individuals.** Publicity is an important means of informing the public and gaining recognition for the MOD and for efforts of individual personnel. However, all personnel should, in their relations with the media, ensure that they do not divulge information that would assist terrorists to target either themselves or other members of the MOD. The following provides some general guidance:

   a. Individuals are always free to decline to give any information to the press.

   b. Private addresses should not be disclosed. Home towns may be specified in such articles as "local boy" stories. Journalists should be advised accordingly when conducting interviews.

   c. Avoid giving ranks and addresses in public notices in the personal and social columns of newspapers.

   d. Individuals who feel that they are at particular risk by virtue of the branch of the MOD to which they belong, or because of operational duties they have performed, who have agreed to be involved in a story in a MOD magazine or newspaper, should ensure personally that biographical detail is cleared with them before publication.

2. **Service authors.** Service authors of articles to be published in Service or general magazines and newspapers should be alert to the dangers that could arise from writing stories that include details of Service personnel. For example, articles that connect named personnel with operational incidents should be avoided.

3. **Service publications editors.** The editors of Service publications should take care to avoid inadvertently providing information that could be useful to terrorists. Guidance on security matters is available to editors of Service publications and establishment magazines from MOD and Command Media Ops and security staffs.

4. **MOD associations.** All MOD associations and similar organizations should remind members that some of the information contained in their correspondence and magazines might be of use to terrorist organizations. Recipients of such material should be warned that it should, therefore, be treated and disposed of with care.

5. **Honours and awards.** Staff responsible for gazetting and publicising honours and awards are to ensure that, where necessary, suitable arrangements are made to protect the anonymity of individuals whose background makes them especially vulnerable to terrorist attack.

6. **Publication of the names of those holding official appointments.** The following guidance should be adhered to when considering the release of information of those holding official appointments for inclusion in such publications as commercial directories:

a. The names of those at one-star and below are not normally to be released.

b. Regardless of rank, the names and telephone numbers of those holding appointments in the following categories are not to be released:

(1) Intelligence.

(2) Security (where "Security" is included in the post title).

(3) Counter Terrorism.

c. The provisions of 6.a. above do not apply to:

(1) The Defence Corporate Communications organization.

(2) The Defence Export Services Organization.

7. Any other organization that feels that it deserves special status should, consult D Def Sy through the chain of command.

ANNEX E TO SECTION V TO CHAPTER 7

SURVIVAL IN HOSTAGE SITUATIONS

1. Good personal counter terrorist security and anonymity as described elsewhere in the Defence Manual of Security (JSP 440) are the most effective counter measures to avoid targeting and therefore becoming a victim in a hostage or kidnapping situation.

2. Very few military personnel have been kidnapped or held hostage in the past. However there has been a general increase in kidnapping world-wide and there is therefore an increased possibility of military personnel being held as human shields during humanitarian or peace keeping operations.

3. The security advice contained in this Annex is based on the Foreign and Commonwealth Office (FCO) Brief Guidance Notes on Personal Protection Measures Overseas.

General

4. Nobody can predict when, where or against whom terrorists will strike. Although senior officers may be singled out as an attractive target, because of their high publicity value, all ranks must be aware of the danger. For this reason it is important to retain anonymity within the local community and to keep a low profile, especially when off duty. Service personnel must make every effort to keep up to date, through their designated overseas security authority (this must be decided prior to deployment), with any changes to the threat. This is reflected in the Overseas Terrorist Threat Assessment List (OTTAL), which is disseminated by MOD D Def Sy. However, despite a thorough awareness and appreciation of the terrorist threat, together with the application of preventative measures, kidnapping can still take place, therefore all ranks should be aware of survival techniques if taken hostage.

5. Once captured the hostage is on his or her own, usually in total isolation. Their immediate reaction and subsequent behaviour during captivity can be vital in leading to their eventual release unharmed. The following notes have been prepared from debriefings of hostage victims.

Moment of Capture

6. This is generally one of the most critical and dangerous parts of the abduction phase. Any sudden or unexpected movement, noise or cry for help is likely to provoke a violent response from the terrorist, which could prove fatal to the captive. In a hostage situation tension will remain high until the terrorists are sure that they are in control. They will attempt to gain a psychological advantage by putting the captive on the defensive.

Resist or Submit?

7. Whether to resist or surrender to kidnappers must remain a personal decision. You should weigh carefully the danger of resistance in the face of what may be overwhelming odds. If you decide not to resist, assure the abductors of your intention to co-operate, particularly during the abduction phase. Remember that resistance is extremely risky because the terrorists are already mentally prepared to meet this contingency and are acting under a great deal of tension during the first few moments of the operation.

Blindfolds, Gags and Drugs

8. It is important to realize that terrorists want hostages alive. While they may use blindfolds, gags or drugs at the time of the abduction, you should not be over-alarmed, pressured or provoked into resisting. Resistance is likely to result in the terrorists using more extreme measures.

Stay Alert

9. Try to occupy your mind by noting sounds, direction of travel, passage of time, conversations of the terrorists and any other information which later could lead to their capture and conviction.

Living Conditions

10. The living conditions of hostages vary greatly from incident to incident. In general hostages are detained in cramped conditions and in isolation. There will usually be a complete lack of privacy and conventional toilet facilities may not exist. Maintaining dignity and self-respect under such conditions will be difficult, but such standards are important for survival.

Fear

11. Fear is the most important tool of terrorists. They use it to control, intimidate and wear down the hostage, negotiators and anyone sympathetic to the victim's plight. Fear may be further induced by the captors loading and unloading weapons in the presence of the hostage, displaying excesses of temper, resorting to physical abuse and staging mock executions. Fear of dying is very real and it can become overwhelming, particularly during the early stages of captivity. Although death is a possibility remember that, statistically, the odds favour a hostage being released.

Time

12. Experience has shown that the more time that has elapsed the better are the chances of the hostage being released or rescued. For this reason, although the passing of time in captivity is depressing, it is to the hostage's advantage.

Boredom

13. To ward off the effects of boredom and keep up morale, the hostage must discipline himself to take daily physical exercise and engage in creative mental activity such as reading, writing or any other pursuit that exercises the mind. Because of the likely cramped space, physical exercise may be reduced to running on the spot, push ups and sit ups. Isometric exercises may have to be used to overcome cramped space or physical restraints.

Illness

14. A side effect of captivity for some hostages is illness caused by inadequate meals or poor diet. Gastro-intestinal upsets or constipation may also be suffered. Though such symptoms may be unpleasant they do not generally threaten life and the hostage should not hesitate to complain to the terrorists, who normally want to keep their hostage alive and at least reasonably well.

Rapport

15. It is important for the hostage to establish an early rapport with the captors. Studies have shown that the more human their victims appear, the more difficulty the captors will have in carrying out threats of violence against them. The display of family photographs or discussions about children and family matters have, occasionally, been instrumental in saving the lives of hostages. Of course, you must avoid giving the terrorists any information, which they could use later to their advantage. This is a matter of fine judgement, particularly for female hostages, and care should be taken not to give the terrorists the wrong impression by becoming too familiar.

Rescue or Release

16. Most hostages who die are killed during rescue attempts. So it is crucial for hostages to be particularly alert, cautious and obedient if they suspect that such an attempt is close at hand. The terrorists may be extremely nervous during any negotiations, especially if the process is long and drawn out. As the central figure in any rescue attempt, the hostage must avoid all sudden moves, which would invite reaction from the rescue force as well as from the terrorists. The natural impulse to stand up and run must be resisted as it could easily be thought to be the action of one of the terrorists by the rescue force. The hostage's safest course is to drop immediately to the floor and lie as flat as possible. Carry out any request by the rescue force and remember that the rescuers may not know you initially and they are trained to treat everyone as a suspect until positively identified.

This page intentionally left blank

SECTION VI TO CHAPTER 7

LEAVE AND TEMPORARY DUTY VISITS TO NORTHERN IRELAND (NI) AND THE REPUBLIC OF IRELAND (ROI)

General

07601. In order to protect Service personnel and to prevent the Security Forces becoming involved in avoidable additional effort and danger, restrictions exist on the taking of leave in Northern Ireland (NI) and the Republic of Ireland (ROI). Service personnel should be well aware of the inherent risks involved and that while the security situation in NI remains unsettled they would not wish to visit either country without good reason. Restrictions on personnel taking leave and visiting on temporary duty have therefore been introduced and it is essential that the rules and guidance laid down in this Section are observed. By doing so unnecessary administrative effort and disappointment to individuals will be avoided. It is the responsibility of the HOE to ensure that only eligible personnel are granted permission to visit NI or the ROI whether on or off duty.

Leave in NI

07602. Regardless of any change in conditions of eligibility, notification or reporting, the following is to be observed by **all** Service personnel taking leave in NI.

a. When on leave civilian clothes are to be worn at all times. Service personnel wishing to wear uniform in NI for a specific occasion, e.g. a wedding, are also to seek permission from the senior officer of the relevant Service in NI, when notifying leave details to the relevant Brigade HQ. Civilian clothes are to be worn when travelling to and from NI.

b. Service style or issued clothing and equipment, e.g. Service issue raincoats, overcoats, holdalls, Service ties, blazers or badges, are not to be worn or carried. Baggage labels showing Service particulars and badges and stickers on vehicles showing military connections must be removed.

c. Privately owned vehicles with registration plates (e.g. NATO registration) that could identify the occupants as being connected with the Service are not to be taken to NI.

d. Regulations for firearms, including air and gas weapons, are published periodically in DCIs/GAIs. HOE are to ensure that these regulations are brought to the attention of personnel intending to travel to NI.

e. Personnel should not indicate that they work for the Services or talk about their job or place of work.

Leave Travel to NI - General

07603. This section provides the framework of rules that apply to all or part of NI according to the assessed security situation at the time. Where the application of the rules vary or change for a specific reason this will be updated by signal from HQNI through MOD D Def Sy and PSyAs and Command security staff will be notified accordingly.

Authority for Leave Visits

07604. Authority for Service personnel to take leave in NI rests with the Brigade HQ of the area to be visited. Notification for all such leave visits is mandatory and is to be submitted in accordance with the following paragraphs. The rules apply to all Service personnel, except those stationed in NI, who are subject to special additional regulations. There will occasionally be periods of time when leave will not be allowed; in such instances the Brigade HQ will advise establishments accordingly when the leave is requested. MOD civilian staff are not subject to these notification rules.

Eligibility for Leave Visits

07605. There are three states that affect the eligibility of Service personnel wishing to take leave in NI and these will vary in accordance with the current security situation. The states affecting eligibility are:

a. **Condition Normal.** No restrictions on visits.

b. **Condition Restricted.** Service personnel may only take leave in NI if the individual concerned can fulfil at least one of the following criteria:

(1) Was domiciled in NI up to the time of joining the Service.

(2) Is married and the spouse would normally be domiciled in NI.

(3) Has a parent or first relative, i.e. brother, sister or child, domiciled in NI.

(4) Has urgent private affairs in NI that cannot be postponed and the requirements cannot be met by a meeting outside NI or by correspondence. Any cases of doubt are to be referred to security staff.

(5) Has been sponsored by an individual currently on the posted strength of a NI unit. (The leave notification signal is to include the rank, name and unit of the sponsor and Service accommodation address, only a mess or Service families accommodation address is acceptable).

c. **Condition Nil.** No leave visits.

07606. The prevalent state existing throughout NI under the current assessed security situation is **Condition Restricted.**

07607. As the security situation in NI changes it is sometimes necessary to place areas out of bounds at short notice to all Service personnel, therefore, permission to take leave may be withheld despite correct notification of the intended leave period and the eligibility of the individual concerned. Establishments will be advised accordingly.

Application for Leave Visits

07608. All Service personnel wishing to take leave in NI are to make an initial formal application through their HOE. MOD civilian staff should inform their HOE and obtain a copy of the security briefing at Annex A. HOE are to ensure that Service personnel are eligible to take leave and meet the criteria detailed in paragraph 07605. Leave details are then to be forwarded to the relevant Service authorities in NI using the signal format shown at Annex B. A map showing NI Brigade areas is at Annex C. No signal is required for MOD civilian staff.

07609. HOE are responsible for ensuring that the notification by signal provides at least 21 clear days notice before the intended leave visit. Signals should be sent ROUTINE, except in compassionate circumstances, when an IMMEDIATE signal is to be sent in addition to the further actions required as detailed at paragraph 07613. Confirmation of receipt must be obtained for all applications. Included in the confirmation will be whether authority is granted or not and whether any specific instructions will apply.

07610. The purpose of the leave notification system is:

a. To give the relevant Brigade HQ the opportunity to assess the risk to the individual and advise the HOE that a visit may warrant postponement or cancellation.

b. To ensure that Service personnel arriving on leave receive an up to date briefing about the security situation in the area(s) to be visited. This will reduce the chances of unnecessary exposure to dangers through ignorance.

c. To provide units in NI with information on the presence of Service personnel, or families, within their area of responsibility. This will allow them to take any appropriate action should the security situation suddenly change.

Leave Addresses

07611. Because of the rapidly changing security situation, Service personnel will only be granted permission to stay at, or visit, private addresses that have been specified for clearance at the time of the signalled application. Any intention to attend wedding services and receptions or christenings etc, must be notified at the time of the original submission and should include additional addresses and intended dates of visits.

Compassionate Leave Travel

07612. When it is necessary to travel to NI on compassionate leave the establishment authorizing the travel is to inform the Brigade HQ in whose TAOR the leave destination is situated. Initial contact is to be made by telephone. However, since telephones lines to NI are insecure, only outline references to the case, i.e. the applicant's name and rough details of the area to be visited are to be given. This is to be followed by an IMMEDIATE signal as outlined in Annex B.

24 Hour Contact Telephone Numbers

HQ	Telephone Numbers	Notes
HQNI	Lisburn Mil 42274 Civil 02892 609274 Brent 20247	Watchkeeper
HQ 3 Inf Bde	Portadown Mil 47590 Civil 02838 360590 Brent 23814	Watchkeeper
HQ 8 Inf Bde	Londonderry Mil 34509 Civil 02871 340509 Brent 27068	G2 Branch Registry (24 hours, try first)
	Londonderry Mil 34208 Civil 02871 340208 Brent 27000	Watchkeeper (use if G2 Registry not available)
HQ 39 Inf Bde	Lisburn Mil 41159 Civil 02892 608159 Brent 20072	G2 Branch (normal working hours)
	Lisburn Mil 41012 Civil 02892 608012 Brent 21017	Watchkeeper (use in silent hours)
RAF Aldergrove	Aldergrove Mil 31340 Civil 02894 421340 Brent 26077	Security Advice Centre (0700-2359 hours)
	Aldergrove Mil 31382 Civil 02894 421382 Brent 26074	Hotel VCP (0001-0659 hours)

Security Briefings

07613. HOE are to ensure that all personnel proceeding on leave to NI receive a personal security briefing using the information at Annex A. Personnel are to be instructed that if they are in any doubt about participation in any activity, out of bounds areas or visits to places of entertainment they are to enquire at the relevant Brigade HQ in whose area they are staying or at the nearest military unit.

07614. In addition to receiving a briefing prior to their departure on leave, all Service personnel will be required to report in person for an additional security briefing, at either the Security Advice Centre (SAC) RAF Aldergrove for RAF personnel, or the R IRISH Battalion TAOR HQ of the area concerned, immediately upon arrival in the Province.

Personnel will be advised of the exact reporting requirement, by signal, to their parent establishment prior to the move. On conclusion of the leave period Service personnel will be required to book out by telephone with the SAC or TAOR HQ. Failure to attend the security briefing may place the individual at increased risk and disciplinary action may be taken against Service personnel who fail to comply.

Failure to Report back from Leave

07615. Should personnel fail to report back from leave, the following are to be informed immediately.

a. **Naval and Army personnel.** The Brigade HQ in whose TAOR the leave has been taken is to be informed by telephone.

b. **RAF personnel.** The SAC RAF ALDERGROVE is to be informed by telephone (RAF Aldergrove Mil 31340, Civil 02894 421340, Brent 26077).

c. **MOD civilian personnel.** The Brigade HQ in whose TAOR the leave has been taken is to be informed by telephone.

07616. All relevant details are then to be sent by IMMEDIATE signal.

Frequent Visitor Status

07617. Brigade HQ staff in NI are authorized to grant the privilege of frequent visitor status to individuals. This privilege permits travel to an agreed leave address without clearance. Notification only is required by signal prior to each journey. Frequent visitor status will only be granted to individuals with a sound security profile. The qualifying criteria includes:

a. The applicant will travel frequently.

b. The destination is an agreed, cleared address in an assessed safe area.

c. The applicant has no history of threats, OOB violations or personal security compromises.

07618. Service personnel granted frequent visitor status will be required to attend an initial security brief with subsequent update briefs at regular intervals. The intervals between update briefs will be at the discretion of the relevant Brigade HQ G2 staff.

07619. A deterioration in the security situation or of specific threats may result in the withdrawal of status at short notice. Any abuse of the privilege will also result in the immediate withdrawal of status.

Travel to and from NI

07620. Service personnel travelling to NI may travel by air to either Belfast International Airport (Aldergrove) or Belfast City Airport (Harbour). Travel by sea must be through the following routes:

a. **Norse Irish Ferries (Liverpool - Belfast).**

(1) **New arrivals.** All Service personnel posted to NI are permitted to use this route but must be met at the Port of Entry (POE) by a unit representative.

(2) **Foot passengers.** Service personnel and their families are permitted to use this service and may be collected by either unit or private family transport. **Under no circumstances is public transport to be used.**

(3) **Green vehicle moves.** Authorization to use this route should be sought from HQNI.

b. **Stena Sealink (Stranraer - Belfast).**

(1) **New arrivals.** All Service personnel posted to NI are permitted to use this route but must be met at the POE by a unit representative.

(2) **Foot passengers.** Service personnel and their families are permitted to use this service and may be collected by either unit or private family transport. **Under no circumstances is public transport to be used.**

(3) **Green vehicle moves.** Authorization to use this route should be sought from HQNI.

c. **P & O Ferries (Cairnryan - Larne).**

(1) **New arrivals.** Service personnel posted to NI are permitted to use this route. It is strongly recommended that a unit representative is present at the POE. Where this is not possible the new arrivals are to be fully briefed, prior to arrival, of their onward journey by the receiving unit.

(2) **Foot passengers.** Service personnel and their families are permitted to use this service and may be collected by either unit or private family transport. **Under no circumstances is public transport to be used.**

(3) **Green vehicle moves.** Green vehicle moves are permitted on this service.

Other routes are **not** to be used.

07621. Personnel travelling to NI on duty visits are normally to travel by air to Belfast International Airport (Aldergrove) or Belfast City Airport (Harbour).

Note: All transport arrangements to and from airports are **to be co-ordinated through the duty visit sponsor. Under no circumstances are personnel to travel in taxis or on other public transport.**

Marriage within NI

07622. Service personnel wishing to marry in NI and who fulfil the conditions detailed in paragraph 07605 should make a formal application to their HOE. Details are then to be sent by CONFIDENTIAL letter to HQNI (SO3 G2(CI)), the Brigade HQ (SO3 G2) of the area in which the marriage and reception is due to take place. RN and RAF (SAC RAF ALDERGROVE) single-Service security staffs with security responsibilities for their personnel in NI should also be included on the distribution. The letter is to be dispatched to arrive at least 30 days in advance of the impending marriage containing the detail required at Annex D.

07623. Personnel who wish to wear uniform during the marriage ceremony may only do so with the prior specific authority of HQNI.

Temporary Duty Visits to NI - General

07624. It is essential that temporary duty visits to NI including participation in Public Military Events (PME) are carefully controlled to ensure that security safeguards and requirements are met. Personnel who have a valid reason to visit NI on official duty are to signal their intentions in accordance with Annex E. PME notification should be made to the Bde HQ (copy to HQNI) in whose TAOR the event is taking place using the proforma at Appendix 3 to Annex I to Section IV of this Chapter.

Duty Visits to Service Establishments and Defence Contractors

07625. As much notification as possible should be given, however, where less than 48 hours remains before the intended visit, signals are to be given a PRIORITY precedence. Operationally urgent, or short notice visits should be notified to HQNI (Attn SO3 GS Visits) by telephone (Lisburn Mil 44206; Civil 02892 625206; Brent Lisburn Mil 21401) followed by a confirmatory signal.

07626. Visits to defence contractors should not be made unless the matter cannot be dealt with by correspondence or by a reference to a departmental head in NI. In all cases the length and frequency of any visit is to be kept to an absolute minimum.

07627. Service visitors requiring to remain in NI overnight will be usually be required to stay in Service accommodation within secure perimeters. Exceptionally, and only with prior approval of HQNI, will Service personnel be allowed to stay in suitable hotel accommodation arranged by the host firm; however, for obvious reasons, this should be avoided if at all possible.

07628. Notification of any duty visit is to arrive in the signal format at Annex E at least 14 days in advance of the intended visit. Prior to embarking on the visit, visitors are advised to contact either HQNI or the relevant Brigade HQ G2 staff for advice on the security situation at the time.

Duty Visits to Civilian Addresses

07629. Notification of duty visits by Service personnel to civilian addresses or accommodation, for example to undertake a resettlement course etc, are to be forwarded to the relevant Brigade HQ arrive at least 14 days before the planned visit.

Duty Visits by Sports Teams

07630. Visits to NI by sports teams will be permitted under Condition Restricted subject to the following:

a. The security situation at the time of the proposed visit.

b. Availability of accommodation at a Service establishment.

c. Visiting teams will be restricted to the confines of Security Force bases throughout their stay.

d. Teams will not be allowed to bring supporters.

e. Financial approval for travel; although every effort is to be made to use Service aircraft.

f. Details of the visit are to be signalled at least 14 days in advance of the intended visit using the format at Annex E.

Carriage of Protectively Marked Documents

07631. Any protectively marked documents that are essential for meetings or briefings etc, are to be sent in advance by the Defence Courier Service (DCS).

Green Vehicle Movements to NI

07632. Standard military vehicles (Green Vehicles) bearing military registration numbers, logos or colour schemes, are subject to special restrictions. Notification of such movements are to follow the format detailed at Annex E, however, signals are to be protectively marked CONFIDENTIAL. Routes should be cleared with HQNI before being included in movement plans.

07633. The accompanying party is to comprise a minimum of two Service personnel who are to wear civilian clothes. Vehicles are to be secured whilst on the car deck of the ferry and are to be thoroughly checked prior to disembarkation.

07634. Escorts will be provided from the ferry port to the ultimate destination in NI. This requirement is to be indicated on the notification signal at Annex E.

Personal Security Briefing

07635. HOE are to ensure that all personnel proceeding to NI on temporary duty receive a personal security briefing using the information at Annex A. Personnel are to be instructed that if they are in any doubt about participation in any activity, require information about out of bounds areas or in bounds entertainment establishments they are to enquire at the relevant Brigade HQ in whose area they are staying or their host military unit.

Leave Travel to the ROI

07636. This section provides the framework of rules and guidance that may apply to all, or part, of the ROI according to the security situation and assessed threat. This policy will be kept under review by MOD D Def Sy taking account of advice from the Defence Attaché (British Military Representative Dublin (BRITMILREP Dublin)). These rules apply only to Service personnel including those stationed in NI who are subject to special additional procedures for leave and travel in the ROI issued by HQNI.

Application for Leave in the ROI

07637. All Service personnel who wish to take leave in the ROI are to make a formal application to their HOE who is authorized to grant such leave in accordance with the criteria and constraints contained in paragraph 07638 and subject to the following:

a. Prior consultation with the BRITMILREP Dublin in cases of doubt.

b. Prior notification, giving appropriate notice, to the BRITMILREP Dublin.

07638. There are three 'states' affecting the eligibility for leave that apply to all, or part, of the ROI and will vary according to the security situation in NI and the assessed threat. These 'states' apply to presence in the ROI and should not be confused with conditions laid down under normal single-Service regulations, for the entitlement to travel at public expense.

a. **Condition Normal.** No restrictions on leave.

b. **Condition Restricted.** This implies that there is some risk involved and that details of all visits will be notified to the Garda Siochana (Police) by the BRITMILREP Dublin. HOE permission should only be given to an individual who has a genuine need to visit the ROI, who has a specific approved address to go to, and who fulfils at least one of the following criteria:

(1) Was domiciled in the ROI up to the time of joining the Armed Forces.

(2) Is married and the spouse would normally be domiciled in the ROI.

(3) Has a parent or a first relative, i.e. brother, sister or child domiciled in the ROI.

(4) Has urgent affairs to settle in the ROI that cannot be postponed and which cannot be met by a meeting outside the ROI or by correspondence. As a guide to the application of this condition by HOE, personnel attending as participants at legal proceedings would be eligible as would a groom or bride (but not their guests) if there is a good reason why the marriage cannot take place elsewhere. Where personnel wish to visit fiancées or partners, the HOE is to be satisfied of the substantive nature of the relationship and the necessity for the visit. Holidays, recreational activities or sport do not qualify for leave under this state. Any cases of doubt are to be referred to the BRITMILREP Dublin.

(5) Is required to travel to the ROI on authorized compassionate leave.

(6) Is serving on a resident tour in NI and is subject to the detailed procedures and controls laid down by HQNI.

(7) Is making a day visit to Dublin under specific arrangements approved by BRITMILREP Dublin and D Def Sy.

c. **Condition Nil. N**o leave visits will be allowed.

*At the time of publication **Condition Restricted** applies for leave to all areas of the ROI.*

Notification

07639. The BRITMILREP Dublin is to be notified by signal when Service personnel are granted leave to the ROI by the HOE. HOE are responsible for ensuring that the notification arrives 21 days before the intended visit, except in compassionate circumstances or, exceptionally, when leave is granted at short notice. The BRITMILREP Dublin will advise if there are any reasons why the leave should not take place, all applications will be acknowledged. The signal should be addressed to BRITMILREP Dublin using the format at Annex F.

Accomodation

07640. Holiday cottages, touring holidays, camping sites and caravan parks will not be approved for leave visits under Condition Restricted. The BRITMILREP Dublin maintains a list of approved hotels for the Dublin area which can be consulted. Hotels North of the River Liffey in central Dublin will not normally be cleared for use. Applicants are warned that they should seek advice from the BRITMILREP Dublin before booking accommodation and making a financial commitment.

Notification

07641. All notifications are to be protectively marked RESTRICTED unless there is reason to afford a higher protective marking. Notification for visits to the border counties of Donegal, Leitrim, Louth, Monaghan and Cavan should also be copied to HQNI BFPO 825, Signal address: NORIRELAND and for information to single-Service security staff with responsibility for personnel in NI.

Briefings

07642. Before Service personnel go on leave to the ROI, the HOE is to ensure that they are briefed by a member of the establishment security organization using the information contained in Annex G.

07643. Events may occur during a visit that would make consultation with the BRITMILREP Dublin necessary e.g. where an individual has been granted compassionate leave to visit a sick relative who subsequently dies and the need to attend the funeral arises or when an individual is sick at home and liable to remain in the ROI following leave expiry date. Individuals are to be briefed to consult the BRITMILREP Dublin should such a change of circumstances occur. Service personnel are therefore to be in possession of the BRITMILREP Dublin telephone number when proceeding to the ROI.

Family Visits

07644. Service personnel are encouraged to adopt the foregoing procedures when members of their families are planning to visit the ROI unaccompanied by them.

Recall Procedure

07645. The notification procedures above will ensure that the BRITMILREP Dublin is in a better position to provide assistance in the event MOD decide to order the recall of all Service personnel on leave in the ROI. In the event of recall, those responsible are to ensure that OHMS envelopes or similarly indicative communications or telephone calls are not sent or made to individuals on leave in the ROI.

Failure to Report back from Leave

07646. Should personnel fail to report back to their establishment after leave in the ROI the BRITMILREP Dublin is to be informed immediately by signal.

Travel to the ROI

07647. Service personnel and their families entitled to travel at public expense are, as a security precaution, to be given the option to pay the full cost of the journey to and from their establishment in the UK and their leave address in the ROI and reclaim the full cost of the fare in lieu of the exchange of warrants covering the UK rail journey, sea crossing and any rail movement within the ROI. **Leave travel to the ROI through NI will only be granted in exceptional circumstances and requires the specific authority of HQNI.**

Temporary Duty Visits to the ROI

07648. Regardless of the leave condition in force, all visits to the ROI by Service personnel on temporary duty require specific prior authorization by the BRITMILREP Dublin. Applications for temporary duty visits should be made giving full details of the proposed activity by letter or by signal using the format at Annex H. Visits by Service aircraft are normally covered using the Diplomatic Clearance (Dipclear) process and the

security brief at Annex I applies. Activities that fall under the category of temporary duty visits include:

a. Visits by HM Ships. Arranged through CINCFLEET (Fleet Programmer), MOD (Naval Staff Directorate) and BRITMILREP Dublin who promulgates General Instructions for visits by HM Ships. Security advice for HM Ships visiting the ROI is issued by FOSF prior to each visit.

b. Visits to Irish Defence Force units.

c. Visits to Defence Contractors.

d. Resettlement courses. Full notification is needed to ensure that the accommodation (often needed for up to 4 weeks or more) is properly booked and cleared.

e. Representational sport.

(1) Under Condition Restricted individuals wishing to play as a member of a civilian team should always seek guidance from the BRITMILREP Dublin before declaring their availability to the team manager.

(2) Applications for participation by Service teams should always seek preliminary guidance from the BRITMILREP Dublin before declaring availability.

f. Adventurous training in the ROI is not usually permitted. Specific proposals should be discussed with the BRITMILREP Dublin before making any financial commitments.

g. Public Military Events (PME). Invitations to Service organizations, including bands and display teams will normally be channelled initially through the BRITMILREP Dublin. Agreement to participate should not be given to sponsors until authorization has been obtained. PME notification should be made to the BRITMILREP Dublin using the proforma at Appendix 3 to Annex I to Section IV of this Chapter.

Accommodation

07649. BRITMILREP Dublin holds a list of approved hotels for the Dublin area. Bookings should not be made through the Central Hotel Booking Service and care should be taken to avoid compromising MOD or Service connections when making reservations.

Personal Security Briefing

07650. A personal security brief using the information at Annex I is to be provided to all Service personnel prior to travelling to the ROI on temporary duty. MOD civilian staff should obtain a copy of the security briefing at Annex I.

Establishment Standing and Routine Orders

07651. Personnel intending to visit NI or the ROI are to be periodically warned, using Standing and Routine Orders, of the requirement of this Section. A suggested entry is as follows:

a. All Service personnel and MOD civilian staff, intending to visit NI or the ROI either on leave or temporary duty, are to read and comply with the contents of Section VI to Chapter 7 of JSP 440.

b. Application details and specific advice can be obtained through the ESyOs and leave administration staff.

This page intentionally left blank.

ANNEX A TO SECTION VI TO CHAPTER 7

BRIEF PRIOR TO VISITING NORTHERN IRELAND (NI) ON LEAVE OR DUTY

1. This brief is to be provided to all personnel prior to travelling on leave or duty to NI.

2. When on leave in NI civilian clothes are to be worn at all times. Civilian clothes are also to be worn when travelling to NI, personnel serving on temporary duty are to wear civilian clothes when off duty and outside the boundaries of their establishment.

3. Military style or issued clothing and equipment (e.g. raincoats, overcoats, holdalls, Service ties, blazers and badges are not to be worn or carried. Baggage labels showing Service particulars are to be removed.

4. Privately owned vehicles with registrations (e.g. NATO) that could identify the occupants as being connected with the Services are not to be taken to NI. Badges and stickers showing Service connections are to be removed.

5. Firearms regulations, including air and gas weapons, are different in NI, further advice can be obtained from: Royal Ulster Constabulary, Explosives and Firearms Licensing Department, RUC Lisnasharragh, Montgomery Road, Belfast, BT6 9JD.

6. Personnel are to exercise discretion at all times, maintaining anonymity about any MOD or Service connections.

7. Disturbances and politically motivated events are to be avoided at all times. If personnel are in doubt about participation in any public activity, they must contact the Brigade HQ in whose area they are staying or at the nearest military unit.

8. Personnel are forbidden to take part in any public activity that may aggravate the security situation by provoking violence or increasing tension in the local community.

9. Service personnel are not to use public transport, including taxis from airports or ferry ports. Unless travelling in their own vehicle they should ensure that they are met at either the ferry port or airport.

10. Personnel should ensure that they have contact numbers for the unit or relatives they are visiting, as well as loose change or phone cards to make telephone calls.

11. All orders received from the Security Forces (whether police or military) are to be complied with regarding movement or behaviour while in NI.

12. Service personnel will be given a security briefing on arrival in NI and should be aware that failure to follow the briefing provided is likely to result in disciplinary action.

ANNEX B TO SECTION VI TO CHAPTER 7

NORTHERN IRELAND LEAVE - SIGNAL FORMAT

To:	3 INF BDE PORTADOWN	}
	8 INF BDE LONDONDERRY	}(Note 1)
	39 INF BDE LISBURN	}
Protective Marking:	RESTRICTED (Note 2)	
SIC:	WAI	

NORIRELAND LEAVE

A. Service number, rank, name, initials.

B. Ethnic appearance (Note 3).

C. Any significant distinguishing features or marks.

D. Establishment or unit including the full civilian and military contact telephone numbers and extensions of relevant leave administration staffs.

E. Leave address in NI and telephone number if available.

F. Name, relationship of the householder in E above to the applicant.

G. Leave dates (inclusive of arrival and departure dates).

H. Route with method of travel, to include flight or ferry timings (when known) otherwise approximate timings are to be given.

I. Dates and location of previous tours in NI (if applicable).

J. Dates and location of previous leave visit to NI (if applicable).

K. Any other relevant information that may assist the relevant Brigade HQ in assessing eligibility for leave.

NOTES:

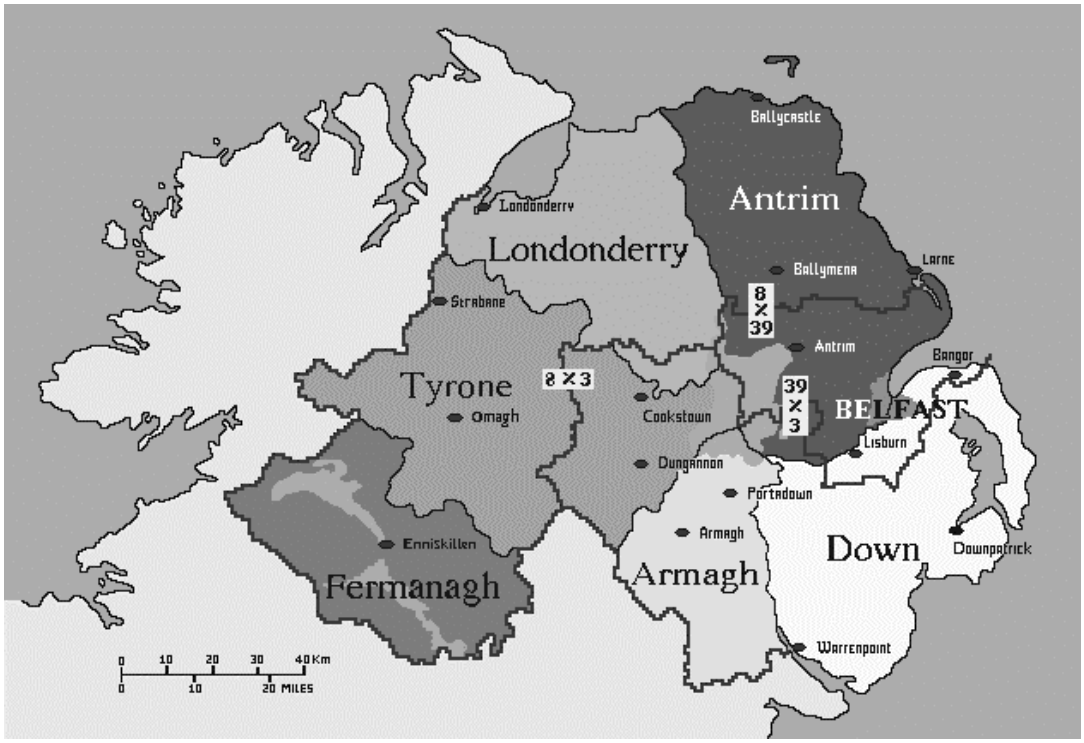
Note 1: The Brigade HQ in whose Tactical Area of Operations (TAOR) the leave destination is situated.

Note 2: The signal is to be protectively marked RESTRICTED, unless the text requires a higher protective marking.

Note 3. Ethnic Appearance Identity Code (IC) 1 White European; 2 Dark European; 3 Afro Caribbean; 4 Asian; 5 Oriental; 6 Arab; 0 Unknown.

ANNEX C TO SECTION VI TO CHAPTER 7

MAP OF NI BRIGADE AREAS



This page intentionally left blank

ANNEX D TO SECTION VI TO CHAPTER 7

DETAILS REQUIRED FOR IMPENDING MARRIAGE IN NORTHERN IRELAND (NI)

1. The details listed below are to be sent by CONFIDENTIAL letter to the Bde HQ in whose TAOR the wedding and reception is taking place at least 30 days in advance of the impending marriage:

a. Service number, rank, name, initials, ethnic appearance[1] and any significant distinguishing marks or features.

b. Names of immediate family accompanying on visit.

c. Unit.

d. Leave address in NI, with telephone number.

e. Name and relationship of occupant at leave address.

f. Dates and location of previous leave visits to NI (if applicable).

g. Name of intended spouse.

h. Duration of visit.

i. Date of wedding.

j. Location of wedding.

k. Location of reception.

l. Complete list of names and addresses of guests.

m. Travel arrangements.

---

[1] Ethnic Appearance Identity Code (IC) 1 White European; 2 Dark European; 3 Afro Caribbean; 4 Asian; 5 Oriental; 6 Arab; 0 Unknown.

n. Names of local businesses involved, e.g. vehicle hire firm, photographer, caterers, musicians etc.

o. Dates and location of previous tours of duty in NI (if applicable).

ANNEX E TO

SECTION VI TO CHAPTER 7

NORTHERN IRELAND DUTY VISIT BY SERVICE PERSONNEL - SIGNAL FORMAT

To:	NORIRELAND	
	RAF ALDERGROVE (See Note 1)	
	3 INF BDE PORTADOWN	}
	8 INF BDE LONDONDERRY	} (See Note 2)
	39 INF BDE LISBURN	}
Info:	NORIRELAND (See Note 1)	
	HQ P&SS HENLOW (See Note 3)	
	SNONI (See Note 4)	
Protective Marking:	RESTRICTED (See Note 5)	
SIC:	WAX/YAA	

DUTY VISIT TO NORTHERN IRELAND. HQNI FOR SO3 G3 (VISITS). BDE HQ FOR SO3 G2.

A. Service number, rank, name and appointment.

B. Parent establishment or unit.

C. Service unit or name and address of civilian firm to be visited in NI. A contact telephone number and name must also be provided.

D. Dates of visit and stay in NI, including arrival and departure dates and travel details.

E. Details of arranged accommodation.

F. Purpose of visit and any other relevant information.

NOTES:
1. For RAF visitors only, if the visitor is of Wg Cdr rank or below and does not intend visiting any other unit or formation other than RAF Aldergrove; then SRAFONI (Sy Servs) will authorize the visit. In this instance RAF ALDERGROVE is to be an action addressee and NORIRELAND an info addressee; the text of the signal is to include "RAF ALDERGROVE FOR SY SERVS".

2. Brigade HQ addressees will be dependent on unit or area to be visited. See Annex C.

3. For RAF visitors only. Insert in text: HQ P&SS FOR OC CSC.

4. For RN visitors only.

5. The signal is to be protectively marked RESTRICTED, unless the text requires a higher protective marking. For visits by Captains RN/Colonels/Group Captains, 1 or 2 star officers the signal is to be CONFIDENTIAL; for 3 star officers and above the signal is to be SECRET.

ANNEX F TO

SECTION VI TO CHAPTER 7

REPUBLIC OF IRELAND LEAVE - SIGNAL FORMAT

To: BRITMILREP DUBLIN

Info: NORIRELAND (See Note 1)

Protective Marking: RESTRICTED (See Note 2)

SIC: WAI

REPUBLIC OF IRELAND LEAVE

A. Service number, rank, name and initials.

B. Ethnic appearance. (See Note 3)

C. Any significant distinguishing features or marks.

D. Establishment or unit to include full civilian and military contact telephone numbers and extensions of relevant leave administration staff.

E. Leave address in ROI and contact telephone number within reach of this address. (See Note 4)

F. Name and relationship of the householder in E above to the applicant.

G. Leave dates (inclusive of arrival and departure dates).

H. Route with method of travel to include flight or ferry timings. When travel is by vehicle the registration number and colour make and type detail is to be provided.

I. Details (including date, time and place) of any public or semi-public functions (e.g. wedding or funeral including church and reception) to be attended should be given.

J. Any other relevant information.

NOTES:
1. Only required if visit includes an address in the border counties of Donegal, Leitrim, Louth, Monaghan or Cavan.

2. The signal is to be protectively marked RESTRICTED, unless the text requires a higher protective marking.

3. Ethnic Appearance Identity Code (IC) 1 White European; 2 Dark European; 3 Afro Caribbean; 4 Asian; 5 Oriental; 6 Arab; 0 Unknown.

4. See paragraph 07640 of Section VI for restrictions on types of accommodation.

ANNEX G TO SECTION VI TO CHAPTER 7

BRIEF PRIOR TO VISITING THE REPUBLIC OF IRELAND ON LEAVE

Introduction

1. All visits to the Republic of Ireland (ROI) by Service personnel on leave require specific prior notification to the Defence Attaché (British Military Representative Dublin (BRITMILREP Dublin)). Notification should be made by signal using the format at Annex F. The following brief is to be provided to all personnel prior to travelling on leave to the ROI.

The Threat

2. Republican influence affects the manner in which Service personnel are perceived in the ROI and may place them at risk if identified. While the security situation in NI remains unsettled, republican terrorist groups retain the capability to target Service personnel on leave or temporary duty in the ROI. Republican influence in the ROI remains significant and some elements of the general public sympathize with republicans in the North and have provided support. Although it is assessed that an attack within the ROI is unlikely, awareness of the presence of identified Service personnel increases the risk. It is more likely that republican terrorist groups would attempt to gain targeting intelligence in order to mount an attack elsewhere. Close Quarter Assassination (CQA) is assessed to be the most likely form of attack if an appropriate target is presented. Additionally, dissident loyalist terrorist groups have threatened attacks against targets in the ROI, in which visitors might inadvertently become involved.

Personal Security Counter Measures

3. Civilian clothes are to be worn when travelling to and from the ROI and Service uniform may not be worn or carried. Military style or issue clothing and items of equipment (e.g. holdalls, Service ties, blazers and badges) are not to be worn, openly displayed or carried when travelling to or in the ROI. Labels and markings that show Service connections are to be removed from baggage. Defence ID cards should not be taken to the ROI but a passport or driving licence may be used for routine identification purposes.

4. Privately owned vehicles with registration plates (e.g. NATO) which identify Service connections are not to be taken to the ROI. Badges and stickers that show Service connections are to be removed. Service personnel are to ensure that they are either met at the airport or ferry port or are fully briefed on their onward route.

Personnel should ensure that they have contact numbers for the relatives they are visiting, as well as loose change or phone cards to make telephone calls.

5. Service personnel should exercise common sense and discretion at all times with the aim of maintaining a low profile and protecting their personal anonymity while in the ROI. Service personnel should be prepared to provide a residential (non-military) address that, if necessary, also matches their credit card address. Disturbances or politically motivated events are to be avoided. Identity as a member of the Armed Forces, is not to be routinely disclosed except to the Irish Defence Forces or the Defence Attaché (British Military Representative Dublin (BRITMILREP Dublin)) or Garda Siochana (Police) in cases of emergency or difficulty. All orders and instructions received from the Garda, Irish Defence Forces or BRITMILREP Dublin are to be complied with regarding movement or behaviour while in the ROI.

6. If, exceptionally, Service personnel on leave in the ROI have a valid reason to travel to NI, specific permission is to be obtained from the BRITMILREP Dublin and HQNI.

7. Any suspicious incidents or approaches are to be reported to the BRITMILREP Dublin and the ESyO on return.

Useful Telephone Numbers:

International Dialling Code for the Republic of Ireland - 00 353

Dialling Code for Dublin – 01 (00 353 1)

British Embassy – 00 353 1205 (within the ROI 01205)

3700 – Switchboard*

3792 – Assistant Defence Attaché

3793 – Leave Enquiries (part-time only)

3878 – Fax (Insecure)

Garda Siochana (Police)	999 or 112
Ambulance	999 or 112

Note* Outside working hours the Embassy Switchboard will connect to the duty officer who should only be connected in an emergency.

ANNEX H TO SECTION VI TO CHAPTER 7

REPUBLIC OF IRELAND TEMPORARY DUTY VISIT BY SERVICE PERSONNEL - SIGNAL FORMAT

To: BRITMILREP DUBLIN

Info: NORIRELAND (See Note 1)

HQ P&SS HENLOW (See Note 2)

Protective Marking: RESTRICTED (See Note 3)

SIC: WAX/YAA

DUTY VISIT TO REPUBLIC OF IRELAND

A. Service number, rank, name and appointment.

B. Parent Establishment or unit. to include full civilian and military contact telephone numbers and extensions of relevant administration staff.

C. Purpose of visit.

D. Irish Defence Force unit or name and address of civilian firm or organization to be visited. A contact number and name of sponsor must also be provided.

E. Dates of visit and stay in ROI, including arrival and departure dates and travel details. (See Note 4).

F. Details of arranged accommodation. (See Note 5).

G. Requirement for wearing uniform and any other relevant information.

NOTES:

1. Only required if visit includes an address in the border counties of Donegal, Leitrim, Louth, Monaghan or Cavan.

2. For RAF visitors only. Insert in text: HQ P&SS FOR OC CSC.

3. The signal is to be protectively marked RESTRICTED, unless the text requires a higher protective marking.

4. Military vehicles, including civilianized military vehicles and RN/RAF/AAC support vehicles, may not be brought to the ROI without special high level approval from the ROI government.

5. See paragraph 07649 of Section VI, BRITMILREP Dublin will provide details of approved hotels in the Dublin area.

This page intentionally left blank

ANNEX I TO SECTION VI TO CHAPTER 7

BRIEF PRIOR TO VISITING THE REPUBLIC OF IRELAND ON TEMPORARY DUTY

Introduction

1. All visits to the Republic of Ireland (ROI) by Service personnel on temporary duty require specific prior authorization by the Defence Attaché (British Military Representative Dublin (BRITMILREP Dublin)). Applications should be made by letter giving full details or by signal using the format at Annex H. The following brief is to be provided to all Service personnel prior to travelling to the ROI.

The Threat

2. Republican influence affects the manner in which Service personnel are perceived in the ROI and may place them at risk if identified. While the security situation in NI remains unsettled, republican terrorist groups retain the capability to target Service personnel on leave or temporary duty in the ROI. Republican influence in the ROI remains significant and some elements of the general public sympathize with republicans in the North and have provided support. Although it is assessed that an attack within the ROI is unlikely, awareness of the presence of identified Service personnel increases the risk. It is more likely that republican terrorist groups would attempt to gain targeting intelligence in order to mount an attack elsewhere. Close Quarter Assassination (CQA) is assessed to be the most likely form of attack if an appropriate target is presented. Additionally, dissident loyalist terrorist groups have threatened attacks against targets in the ROI, in which visitors might inadvertently become involved.

Personal Security Counter Measures

3. Civilian clothes are to be worn when travelling to and from the ROI and Service uniform may only be worn when on duty within Irish Defence Force establishments or when specifically authorized by the BRITMILREP Dublin (e.g. when attending the UNMO course or taking part in a Military Band performance). Service personnel are to wear civilian clothes when off duty and outside the boundaries of an Irish Defence Force establishment.

4. Military style or issue clothing and items of equipment (e.g. holdalls, Service ties, blazers and badges) are not to be worn, openly displayed or carried when travelling to or in the ROI. Labels and markings that show Service connections are to be removed from baggage. Defence ID cards may be taken to the ROI but a passport or driving licence should be used for routine identification purposes.

5. Vehicles with registration plates (e.g. NATO) which identify Service connections are not to be taken to the ROI. Badges and stickers that show Service connections are to be removed. If travelling to the ROI for the first time by vehicle, Service personnel are to ensure that they are either met at the ferry port or are fully briefed on the onward route to the place of duty. Personnel are to ensure that they have contact telephone numbers for their host and BRITMILREP Dublin. Alternatively in an emergency telephone the Garda Siochana (Police) by dialling 999.

6. When driving in the ROI, a suitable road map is to be carried at all times. Unless taking part in an official event, which is sponsored and organized by the Irish Defence Forces and specifically authorized by BRITMILREP Dublin, Service personnel are not to enter the border counties of Donegal, Leitrim, Cavan, Monaghan and Louth. Hitchhikers are not to be picked up. A street map of Dublin can be purchased from most bookshops and stationers. Note that in Dublin City centre, when on foot and North of the River Liffey, Service personnel are advised to remain within the central area bounded by Capel Street - Parnell Street - Gardiner Street Lower. Dublin is a large city with all the usual associated risks including vehicle theft, street crime, mugging and drug abuse.

7. Service personnel should exercise common sense and discretion at all times with the aim of maintaining a low profile and protecting their personal anonymity while in the ROI. Outside Irish Defence Force establishments, Service personnel should behave as tourists and be prepared to provide a (non-military) residential address that, if necessary, also matches their credit card address. Disturbances or politically motivated events are to be avoided. Identity as a member of the Armed Forces, is not to be routinely disclosed except to the Irish Defence Forces or the BRITMILREP Dublin or Garda Siochana (Police) in cases of emergency or difficulty. All orders and instructions received from the Garda, Irish Defence Forces or BRITMILREP Dublin are to be complied with regarding movement or behaviour while in the ROI.

8. If, exceptionally, Service personnel on temporary duty in the ROI have a valid reason to travel to NI, specific permission is to be obtained from the BRITMILREP Dublin and HQNI.

9. Any suspicious incidents or approaches are to be reported to the BRITMILREP Dublin and the ESyO on return.

Useful Telephone Numbers:

International Dialling Code for the Republic of Ireland - 00 353

Dialling Code for Dublin – 01 (00 353 1)

British Embassy – 00 353 1205 (within the ROI 01205)

3700 – Switchboard*

3792 – Assistant Defence Attaché

	3793 – Leave Enquiries (part-time only)
	3878 – Fax (Insecure)
Garda Siochana (Police)	999 or 112
Ambulance	999 or 112

Note* Outside working hours the Embassy Switchboard will connect to the duty officer who should only be connected in an emergency.

THIS BRIEF IS NOT TO BE TAKEN TO THE ROI

This page intentionally left blank

CHAPTER 8

(SPARE)

This page intentionally left blank

CHAPTER 9

(SPARE)

This page intentionally left blank

CHAPTER 10

(SPARE)

This page intentionally left blank

CHAPTER 11

DISCLOSURE OF PROTECTED INFORMATION

CHAPTER 11

SECTION I

DISCLOSURE OF PROTECTED INFORMATION OUTSIDE GOVERNMENT SERVICE (EXCLUDING TO OTHER COUNTRIES (SEE SECTION II))

Introduction

1101. This chapter lays down the principles to be observed when considering the disclosure of protected information to persons or bodies outside the Government service. A MOD civilian (including staff in MOD agencies such as DERA), contractor or member of the Armed Services is to disclose such information to another person or body outside Government service **only when satisfied that the recipient meets, as a minimum, all of the following:**

a. A 'need to know' (eg. because of a contract or other form of agreement;

b. The requirements of the originator or sponsor of the information to receive it;

c. The appropriate level of clearance;

d. The appropriate physical measures to store and control access to the material.

Having been satisfied that the criteria at a. to d. above can be met, the person wishing to disclose such information should finally seek authorization from the appropriate security authority.

1102. These baseline **(minimum)** criteria at respective levels of protective marking are described by the following matrix.

(*Note:* BC (Basic check) and BC + NIB (Basic check + National Identification Bureau) are **not** security clearances)

	REGULAR TOP SECRET	OCCASIONAL TOP SECRET	REGULAR SECRET	OCCASIONAL SECRET	CONFIDENTIAL	RESTRICTED
Need to Know	*	*	*	*	*	*
Originator/ Sponsor consent	*	*	*	*	*	*
Developed Vetting	*					
Security Check		*	*			
BC + NIB				*		
BC					*	*
Physical Measures	*	*	*	*	*	*

Stage 1 - clearance for access to protected information

1103. When an individual needs access to protected information the sponsor must seek the appropriate level of clearance via Principal Security Adviser staff. The submission should be made on the relevant security questionnaire, see Volume 2. There is no objection to the individual completing the form.

1104. If access to protected information will require individuals to be cleared for Developed Vetting early notification will be required as the vetting process may take a considerable time to complete. The normal notification period is 5 months.

1105. Where custody of protectively marked documents is not required, but where protected information may be passed verbally, the sponsor should brief the recipient on security responsibilities at the earliest opportunity. The recipient must also be asked to sign the Official Secret Act (OSA) declaration (MOD Form 134) at this time. The recipient will retain one copy of the OSA form and return the other copy to the sponsor.

Stage 2 - clearance for custody of protected information

1106. Confirmation of an individual's security clearance does not constitute authority for receipt and retention of documents or other material marked CONFIDENTIAL or above outside Government premises. If this is necessary, advance arrangements must be made to safeguard them. Sponsors should approach their Principal Security Adviser's staff confirming that it is necessary to allow the individual to retain protectively marked documents or material outside Government premises, and indicating:

a. The highest protection of the material involved, and

b. The address at which protected material will be kept.

1107. On receipt of this information, Principal Security Adviser staff will:

a. Arrange a visit to brief the individual on security matters including the maintenance of a protected documents register (PDR), supply the appropriate security furniture; the OSA declaration (MOD Form 134) will also be collected if not already acquired by the sponsor;

b. Arrange for security clearance of any staff (secretary or assistant) employed by the individual and who may have access to protected information;

c. Arrange periodic security inspections, and the muster of the protectively marked documents held; a report of each visit will be submitted to the sponsor, with a copy of PDR entries for cross-checking against a record of issues made by the sponsor;

d. Ensure that, on resignation or retirement, all protectively marked papers and security furniture are recovered or destroyed in accordance with appropriate regulations;

e. Provide additional briefing should the individual propose to visit a country to which a special security risk applies (CSSRA), or be visited by a person from a CSSRA, sponsors must report any proposed visits, of which they are aware, to InfoSy(IVCO) or Single Service Principal Security Advisers' staff.

1108. Sponsors must not release protected material to any individual or company until advised by InfoSy(Industry) or Single Service Principal Security Advisers' staff that they may do so.

1109. In support of the baseline requirements, further guidance on disclosure to specific individuals/bodies is as follows.

Disclosure of information

To contractors.

It must not be assumed that a firm is cleared solely because it has undertaken protected work in the past or is currently engaged on classified defence work. Particular care must be taken over sub-contractors, both List X companies and generally.

1110. Security principles for the safe-guarding of information and material bearing a protective marking apply with equal force during contract negotiations and in the course of work against a defence contract. Chapter 12 of this manual contains detailed instructions for contracts' branches and other branches/organisations involved with placing protected contracts and releasing protected information to contractors.

1111. Before entering into any discussions that may involve or lead to a disclosure of information marked CONFIDENTIAL or above, heads of establishments are to obtain InfoSy(Industry) or Single Service Principal Security Advisers approval to deal with the firm(s) concerned, or with named individual(s), even if disclosure of information marked CONFIDENTIAL or above is not expected to be necessary until preliminary negotiations have been completed.

1112. Sponsors are to inform contractors of the protection of individual aspects of work to be carried out by issuing a Security Aspects Letter.

1113. Before releasing any protected information to a contractor's employee an OSA declaration form must have been completed by the proposed recipient.

To university Defence lecturers

1114. The advice of Principal Security Adviser staff is to be sought where a request for protected information is received from a university Defence lecturer who is not directed or controlled by the Ministry of Defence, and no advance instructions have been received from the Secretary Academic Studies Steering Group.

At university courses, study conferences, seminars etc.

1115. Unclassified information to be presented as a paper at a conference etc must receive publication clearance. Authors wishing to present unclassified information in a paper at a conference etc must submit their material for prior publication clearance by the appropriate authority (see para 1138).

1116. Authorization for protected material to be presented at a classified conference is the responsibility of the author and the appropriate research area leader/project manager/owner of the protected information. **It is the conference organiser's responsibility to ensure that the venue is suitable and that those attending are cleared to receive the material being presented.**

To promotion, appointment boards etc.

1117. **Ministry of Defence Civil Service promotion and appointments boards.** Provided reasonable discretion is exercised candidates need not feel debarred from disclosing such protected information as is necessary to give a reasonable account of their work. A candidate has the right to know of the composition of the board and should establish the permissible level of discussion.

1118. **Boards of Civil Service Commission or by other Government departments.** Candidates must beware of disclosing protected information unless they know that the board is authorised to receive it. The Chairman's assurance on this should be sought and, if given, accepted.

1119. **Boards of non-Government bodies (eg, for election to a professional association).** Candidates who are asked to discuss their work, should normally be able to do so without disclosing protected information. Those attending the board should consult DD DefSy(S&T), Principal Security Advisers'staff or the establishment security officer (ESyO) if they consider that they will be unable to give a satisfactory account without breaching disclosure regulations.

To the media

1120. The term 'media' should be taken to cover newspapers and periodicals and other publications (including information placed on the Internet), radio and television films, news-reels, video recording, still photographs, exhibitions and publicity and advertising

of all forms.

1121. No member of the Ministry of Defence (including MOD Agencies) is to allow himself/herself to be interviewed by a representative of the media or communicate with the press on official matters. Any approach must be referred to D News (Press Office), as the sole channel of communication with the media on departmental or official subjects.

1122. Representatives of the media who telephone personnel at establishments, seek appointments with them or arrive without appointment, must be referred at once to public relations officers (PRO) or D News. At outstations they must be referred to the head of establishment, or PRO, who will consult D News before making any statement beyond matters within his local jurisdiction.

1123. The disclosure of information by contractors (eg), in advertisements, press releases or at exhibitions, conferences etc) is governed by DEFCONs 531 and 659. Publication clearance for unclassified information is coordinated by DD DefSy(S&T))/Single Service Principal Security Advisers and their procedures must be followed by the contractor. Anyone approached direct by contractors seeking authority to publish unclassified information related to MOD interests **must** refer the inquirer to his/her local Security Controller.

1124. The procedures outlined above also apply when contractors are seeking approval for the publication of photographs of buildings, apparatus, etc. erected or installed at MOD premises.

1125. Staff are to notify DD DefSy(S&T) or Single Service Principal Security Advisers, through their ESyO, of any apparent disclosure of protected information that comes to their notice in articles, broadcasts, advertisements, or in firms' publicity literature etc.

To local authorities

1126. The "need to know" rule applies with particular force to elected representatives of local authorities, or their associations, if for no other reason than that they are subject to frequent change and their physical security measures are less apparent. The safest course is to impart the minimum information necessary to achieve the purpose and then only in response to legitimate enquiries. Wherever possible protected information should be diluted so that release can be undertaken at unclassified or at most RESTRICTED level.

To members of Parliament (including members of the House of Lords and UK members of the European Parliament)

1127. As a general rule, members of Parliament acting in connection with their

parliamentary duties are not allowed access to information graded higher than RESTRICTED. Access to CONFIDENTIAL information may be authorised by the responsible minister. Where information bearing a protective marking is communicated, the member of Parliament is to be informed explicitly of its marking. When considering access by a UK MEP to UK protected information the minister responsible for authorising disclosure must be satisfied that such information will not be disclosed to MEPs of other nationalities.

1128. In the case of proposals to visit an establishment (or a firm holding a protectively marked contract), where more than one Service or department is concerned, the sponsor of the visit is responsible for ensuring proper interdepartmental consultation.

1129. It is unlikely that members of Parliament will have facilities for the safe-guarding of protectively marked documents. Such information should not be communicated to them in writing without approval from Principal Security Adviser staff.

1130. When a Member of Parliament has to be given clearance for access to protected information in a private capacity - eg, as director of a firm undertaking protectively marked contracts - the Home Office is to be consulted, through the relevant Principal Security Adviser staff.

To Parliamentary committees

1131. The Public Accounts Committee (PAC) and the House of Commons Defence Committee (HCDC) will, at the department's request meet in closed session but all other parliamentary committees admit public and media to their hearings.

1132. Guidance regarding HCDC can be found in the 'Notice for Witnesses' available from the HCDC Liaison Officer in the Secretary of State's Private Office; advice to officials appearing before the PAC is available from D Fin Pol.

1133. The House of Commons clerks/staff are responsible for ensuring that distribution of protected information disclosed to parliamentary committees will be restricted to those persons whom departments have agreed may have access.

1134. Protectively marked material is made available to members only during committee meetings and, on request, in the committee office. Members are not free to remove protectively marked documents. Protected portions of oral evidence and, in some cases other special categories of information bearing descriptors eg, "Commercial", given to a committee in closed session, sidelined by the witnesses in the shorthand writer's transcript, will be excised before evidence is printed (in proof form) and distributed to committee members. The full record will be retained in the committee office for examination by members authorised to have access to it.

1135. The release of TOP SECRET information, to committee members and specialist advisers, is subject, in each case, to approval by the responsible Minister.

On the telephone

1136. Telephone requests for information from callers where the caller cannot be satisfactorily identified, should not be met immediately. The caller should be asked to give a telephone number at which he/she can be contacted, this number being checked before any information is disclosed. If the caller declines to give a number the matter is to be reported to the ESyO. The telephone is vulnerable to scan and intercept and highly insecure.

To commercial organisations for commercial publication (information on names etc)

1137. **General.** The release of information about appointments, duties, telephone number, etc, must be carefully controlled to avoid accumulation to the point where the total should be protected. Information containing names, appointments and telephone numbers allows monitoring of calls by Foreign Intelligence Services (FIS) and identifies individuals likely to be of interest to FIS, ie. talent spotting. The information may similarly be used by terrorists for targeting. Provision of collated data, eg in the MOD Directory, frees FIS resources for other, higher value work. Staff should be on their guard when confronted with apparently innocent requests for information. Approaches should be processed in accordance with sub paragraphs a to f below.

a. **Publications**. The release of official information containing names, appointments, duties and telephone numbers is co-ordinated by the Directorate of Corporate Communications Services (DCCS). Appropriate information will be released to commercial publishers who have established a genuine "need to know" and where publication is seen to benefit the department. The following arrangements apply:

(1) Names, etc, of staff at Captain RN/Colonel/Group Captain/Grade 6 level or below will not normally be released. Any organisation or individual currently providing or invited to provide a commercial publisher with such information should inform DCCS. Approaches by letter, questionnaire, telephone, or personal visit, asking individuals to update published material should similarly be referred to DCCS for action; they should **not** be acknowledged.

(2) The constraints detailed in sub para (1) do not apply where they would be counter-productive to the activities and interests of the Defence Export Services Organisation (DESO) or DCCS.

(3) Names and telephone numbers of officials holding appointments

in intelligence, security (where 'security' is included in the post title) and counter-terrorism are **not** to be released to commercial publishers.

b. **Who's Who type publications.** It is largely a personal decision whether Service or civilian personnel provide information for inclusion. Staff are advised to consider the following before taking such decisions:

(1) The publication may be used by terrorists for targeting purposes. It is therefore unwise to allow inclusion of a private address or telephone number or of outside interests that would enable such organisations to trace the subject.

(2) Details provided may be of value to FIS for talent spotting, particularly if employment on Defence-related work is mentioned or implied.

(3) Such publications are widely used by commercial organisations for sales promotion, etc. Unsolicited pamphlets, leaflets, and salesmen may follow publication of personal details.

c. **It is better and safer not to be identified in such publications.** If individuals choose to provide information, office telephone and room numbers should not be disclosed; in addition officers below one-star/Grade 5 or equivalent should not disclose their rank, branch or appointment. Any association with intelligence, security or counter-terrorism work should **not** be disclosed. See also para 1137 a(1).

d. **Questionnaire**. The style and purpose of questionnaires varies considerably. They may be computer-produced or individually typed; ask astute questions or seek apparently innocuous consumer-survey-type information. They are not always in textual form - in some cases surveys are conducted by telephone. All approaches received at the place of work are to be regarded as being made through official channels. Only where participation is seen to be to the MOD's advantage, and where material sought is unclassified and non-controversial should participation be considered. Cases of doubt should be referred through the local security officer to either DD DefSy(S&T))/Single Service Principal Security Adviser's staff or the ESyO as appropriate.

e. **Salesmen.** Where a salesman attempts to sell defence or other equipment/services through personal contact, staff must themselves decide if it was reasonable for them to have been approached. Line managers and InfoSy(Industry)1 or Principal Security Advisers staff should be informed, in writing, where those contacted believe that the organisation making the approach had no reasonable ground to have information enabling the approach to be made. In such cases, those contacted should establish the salesman's name and telephone number, and the title and address of the parent organisation;

these details should be included in the report so that investigations may be made. In deciding whether to report an approach, it must be remembered that some salesmen employ random dialling on MOD exchanges; in some cases, the telephone numbers of senior staff may be available in commercial publications (see a. and b. above)

f. **BT telephone directories.** Service personnel are strongly advised against the inclusion of their rank in BT telephone directories, for reasons similar to those outlined in b. above.

g. **Use of the office address for receipt of personal mail, etc.** Use of the office address as a receiving point for private mail is at the discretion of individuals and subject to guidance/instructions from local security staffs, eg use of BFPO addresses and mail for single Service personnel. Official address/telephone number should not be disclosed for consumer surveys, on hire purchase or credit agreements, or on similar documents.

Publications

1138. Official permission is to be obtained before any member of the Ministry of Defence accepts any invitation, or enters into any commitment, to publish any book, monograph, article or letter, or to deliver any lecture or speech, or take part in any radio or television programme, or put forward any thesis for a degree, diploma, etc, that:

a. Is on a subject akin to the official duties of the officer concerned or of any public servant; or

b. Otherwise relates to the business of the Ministry of Defence or any former or existing Government department; or

c. Has been or will be compiled from sources to which the officer concerned has access in his official capacity; or

d. Will contain a reference to the author's official position or association with the Ministry of Defence.

1139. MOD Personnel Manual Volume 7 Section 6 and Chapter 3 Annex M and MOD Form 655, describe how permission may be obtained by members of the civilian component of the Ministry of Defence. Service personnel are to refer to the relevant instructions in Queen's Regulations. Permission is not required for a lecture, speech or publication that is intended solely for a purely Government organisation or conference, or for attendance at a meeting of a scientific or technical organisation at which a contribution to discussion may be made. Staff must, however, guard against unauthorised disclosure of official information on these and similar occasions and observe the normal precautions for safeguarding protectively marked information. Particular care

is to be exercised when officials are attending formal and informal discussions at conferences, learned societies, professional institutions, exhibitions and receptions where officials of countries presenting a special security risk may be present.

Careless talk

1140. Careless talk is always potentially dangerous - the circumstances are immaterial. To deny or express doubt about the statement of another person may be as dangerous as a positive statement of information. Protected matters are not to be discussed in places where conversation may be overheard by unauthorised persons or even by persons known to be reliable but who do not have a need to know. Particular care is to be exercised in office lifts, canteens and washrooms and even in official cars, as well as in public places such as hotels, public houses, trains and buses. There are many people such as cleaners, canteen assistants, drivers, messengers, porters and maintenance staff employed in Government departments whose presence is familiar and easily disregarded but they have a minimum security clearance and have no 'need to know', they should not, therefore, be entrusted with protected information.

Chain letters

1141. It is for individuals to decide whether they wish to become involved in such letters, but they are advised for security reasons not to do so. Attention is drawn to the need to avoid any unnecessary linkage between individuals, official appointments and/or addresses. Participation in such letters could increase the terrorist threat to an individual and their family. Official resources are not to be used, eg stationery, typing, duplicating, communications and transit services.

Aerial surveys by foreign firms

1142. An application for a foreign registered aircraft to carry out aerial survey or other similar flights over the United Kingdom would normally be submitted to the Department of Trade, who after appropriate enquiry would submit it for clearance to the Secretary, Defence Press and Broadcasting Advisory Committee (Sec/DPBAC). Any application, from whatever source, received directly within the Ministry of Defence, should be referred to Sec/DPBAC.

Unsolicited mail

1143. Frequently unsolicited mail, from various sources, is directed at individual members of staff requesting such items as:

a. photographs;

b. autographs;

c. personal data for inclusion in obscure publications;

d. the use of an individuals's bank account for a "business venture".

In all such cases, staff are advised not to respond. Should staff receive requests from such sources, they should refer the matter to their ESyO for advice/action as necessary.

Security of official maps, charts, plans, air photographs (including air photo-mosaics and films and diagrams)

1144. To ensure that official maps, charts, plans, air photographs (including air photo mosaics and films) and diagrams which are made available to the public meet the legitimate needs and interests of their users, without prejudicing the safety and security of sensitive MOD establishments and installations, staff should refer to the guidance at Annex C. If there are any problems concerning sensitive sites, relating to this subject, the ESyO/USyO should refer the matter to the relevant Principal Security Adviser for advice.

SECTION II

RELEASE OF PROTECTED INFORMATION TO OTHER COUNTRIES

Introduction

1145. These instructions set out the policy, principles, controls and procedures for the release of protected information to Governments, companies and individuals of other countries, by the UK Government and UK companies. These instructions should be brought to the attention of all concerned, and any enquiries about the policy should be referred to Principal Security Adviser staff. **It should be noted that the UK adopts a policy of PROTECTIVE MARKINGS and DESCRIPTORS for its material based upon the consequences of its COMPROMISE in general, whereas other countries CLASSIFY their material on the grounds of National Security. In the UK system there is no unique indicator that a National Security aspect is present, eg. a document marked CONFIDENTIAL - MANAGEMENT may be so marked for National Security reasons as well as Management reasons**.

Policy

1146. The policy for the release of military information is laid down by the Director General International Security Policy (DGISP). The word 'Military' is deemed to encompass all 'Defence' information.

1147. The main object of the policy is to strike a balance between the requirements of security and of the perceived benefits of political, economic or other factors.

1148. A table of recommended release levels (Table 'X') is issued and kept up to date by DESP 2. The contents of Table 'X' are very sensitive and the distribution of it is strictly limited. Any queries on Table 'X' should be addressed to the DESP 2 Sec2.

Principles

1149. Information is released on a Government to Government basis or by industry with UK Government approval, to the Government, industry or individuals of another country. Visiting military/personnel or defence contractors' personnel with suitable credentials and security clearances are eligible to receive visual or oral information on a need to know basis on behalf of their Governments. Once approval for release has been granted, material is to be transferred in accordance with instructions in paras 1160 to 1180.

1150. Information should not be disclosed to other countries unless the Release Authority (see paragraph 1162) is satisfied in respect of both the recipients' "need to

know" and their ability and intention to safeguard that information. The criteria to be used to judge whether release should be permitted should include the following:

a. The protective marking or classification of the material concerned.

b. The Table 'X' release level of the recipient country.

c. The recipient country's role as an ally or otherwise.

d. The probability of its contributing to the defence of Western democracy in terms of research and development, manpower or production.

e. The need for the recipient country to receive this information in order to assist it to contribute to the defence of Western democracy.

f. The chances of the information being compromised.

g. The military or technical value of the information to a potential enemy if it were to be compromised.

h. The advantages to UK in political, military or economic terms over the risk to national security.

These criteria, however, may be amended by special agreements between the United Kingdom and other countries or such other special considerations as those referred to below.

1151. A sponsor branch must be aware of the ownership of the information and must ensure before disclosure that the owner agrees to disclosure. This applies to owners both within and outside the United Kingdom. Thus, the Department should not release information that is the property of, originates in, or is of important interest to, another Department without the latter's consent. Similarly no information which is the property of a private individual or contractor should be released without their consent, and the United Kingdom should not release to a third country information that is the property of another country without the latter's concurrence.

1152. Cost data should not be released without the approval of the appropriate finance or administrative branch since it may be prejudicial to subsequent tendering, international collaborative sharing, commercial, sales or project interests.

1153. Protected information, patent rights, and information of a privately-owned nature which might not be protected under patents, is to be safeguarded as far as possible when released to other Governments. All documents, except those certified for UNCLASSIFIED release, supplied to other Governments should bear one or more of the Conditions of Release stamps or labels referred to in para 1168 and Annex A. Copyright queries should be addressed to MOD Library Services Crown Copyright

Section.

Control of the release of protected information

1154. In the context of these instructions, the term "information" means information about Defence related items including equipment and documentation which:

a. Arises from, and is directly or indirectly related to, any Government contract subject to DEFCONs 531 and 659, and/or

b. Arises from a defence-related private venture funded activity, aspects of which may warrant protection in the national interest, albeit the activity is not governed by standard conditions of contract or subcontract.

1155. There are political, security and in some cases commercial factors which must be considered prior to any agreement to export defence material. On a day to day basis, approval for the release of protectively marked information and hardware overseas is obtained through the Arms Working Party (AWP) (made up of Equipment Security Branch, DD Def Sy(S&T) and various members of the DIS as appropriate, using the Form 680 procedure.

1156. In addition to the MOD, the other Government departments involved in control are:

a. The Foreign and Commonwealth Office (FCO) which advises on political considerations.

b. The Department of Trade and Industry (DTI) which operates the export licensing system.

c. HM Customs and Excise which enforces the controls on the import and export of goods.

1157. The legal authority controlling the release of official information is the Official Secrets Act 1989.

1158. The Import, Export and Customs Powers (Defence) Act 1939 and the Customs and Excise Management Act 1979 govern the export of goods from the UK. The regulations which currently control the export of goods are contained in the current Export of Goods (Control) legislation for military goods and in the Dual-use and Related Goods (Export Control) legislation for other controlled goods.

1159. Prior to the export of licensable defence material, the provision of an export licence from DTI is required. The types of export licence that may be issued are:

a. Individual Export Licence (IEL).

b. Open Individual Export Licence (OIEL).

c. Open General Export Licence (OGEL).

Procedures

1160. This section sets out the procedures to be followed by divisions and branches for the release of information to other countries and is based upon the principles and policies detailed in the preceding paragraphs.

1161. The objects of the procedures are:

a. To ensure that no information is disclosed without proper authority and that where releases are authorised the proper safeguards against unauthorized transfer to third parties are imposed.

b. To ensure that the agreements with other nations about the release of information of overseas origin are not broken.

c. To achieve uniformity of practice within the Ministry of Defence on release of information.

d. To ensure that adequate records are kept of information released.

Release authority

1162. Authorization to release military information overseas will depend upon the content of the information and the country to which it is to go.

a. For certain releases, the Release Authority is the Head of Establishment responsible for that information. Certain powers of release have been delegated also to Commanders-in-Chief, Heads of Service Missions and Service Liaison Staffs, Defence Attaches and Advisers and Commandants of Service Schools. The levels to which members of either of these groups may release are set out in Table 'X' (but see para 1166 in respect of the USA).

b. Release at other levels is subject to prior consultation with the appropriate Principal Security Adviser staff and the following table shows who should be consulted:

Srl	Area	Information on General Military Matters	Information on Equipment	Info. on Technical Security
(a)	(b)	(c)	(d)	(e)
1	Royal Navy Delegated to	Area Security Staff	ACDS OR(Sea) D Def Sys ESB	ISG DD DefSy(S&T) / Command HQ
2	Army Delegated to	Principal Security Adviser	DG of Equipment ESB	DD DefSy(S&T) / Command HQ
3	Royal Air Force Delegated to	Principal Security Adviser	ACDS OR(Air) DG of Equipment ESB	DD DefSy(S&T) / Command HQ
4	Intelligence	CDI	DI(AC)	
5	Technology Transfer		DI(AC)	
6	Cryptographic Matters		CESG/GCHQ	
7	Nuclear Matters		Sc (Nuc) 1	

In cases of doubt, DESP 2 or Principal Security Adviser staff must be consulted.

1163. Acting as the agent of the Release Authority, the Defence Research Information Centre (DRIC), is the prescribed routine channel for the transmission overseas on initial distribution and in, response to specific requests, of Ministry of Defence Scientific and Technical Reports. The DRIC obtains technical policy, patents, commercial and security clearances and is responsible for affixing the appropriate conditions of release. DRIC maintains a record of releases made and can furnish such information on request.

1164. The release of ATOMIC, COMSEC, EMSEC, ECLIPSE, INTELLIGENCE and CHOBHAM ARMOUR information is not delegated to divisions and branches and is the subject of special rules; further information may be obtained from Table 'X' or the appropriate Principal Security Adviser.

1165. The prefix "UK" must be added to protective markings on all hard copy documents to be passed to other countries. However, in formal signal messages transmitted over the Defence Communications Network, the prefix "UK" is not recognised. Therefore, staff must only apply the appropriate protective marking and use the term "UK CLASSIFIED RELEASED IN CONFIDENCE" as the first words of the text. If in doubt as to the correct release instructions for overseas messages, staff should initially contact their local COMMCEN staff for advice.

1166. The United States does not appear in Table 'X' and sponsor branches may, with the consent of the release authority and the owner of the information, release protectively marked information (excluding that detailed in para 1164 for which specific rules, detailed in Table 'X' apply).

1167. When a release proposal by a sponsor branch outside the Defence Export Services Organisation has a current or potential "Sales" implication, the appropriate Regional Marketing Directorate (RMD) should be consulted.

Conditions of release

1168. When information is released overseas the recipient country should be advised of "The Conditions of Release" which may vary according to the reasons for disclosure. The appropriate "Conditions of Release" are to be shown on all protectively marked and UNCLASSIFIED documents released to all overseas recipients either by means of a rubber stamp or a label (see Annex A). In some cases it may be necessary to write specific 'Conditions of Release', if those specified in Annex A do not completely meet the requirement; in such cases the advice of the appropriate Principal Security Adviser staff is always to be sought.

1169. When the release or disclosure is to be made by a contractor, it will be the responsibility of the sponsor branch to issue clear instructions to the contractor to ensure that:

i. There can be no doubt about what information may be released.

j. The appropriate Conditions of Release labels or stamps are affixed to documents before release.

k. Documents are despatched via the sponsor branch who should arrange transmission through approved Government to Government, or other approved channels.

l. In the absence of a sponsor branch, the appropriate RMD should be used.

1170. All releases of protected information to overseas nationals or to their

representatives should be systematically recorded by sponsor branches, or the appropriate RMD.

1171. Release of protected information to a foreign national (eg a representative of an overseas company) should be regarded as release to that individual's country of origin.

Defence Export Services Organisation (DESO) - clearance procedures

1172. The procedures within the DESO for dealing with enquiries from firms and potential customers regarding clearance for the promotion and sale of British defence equipment overseas are set out in "DESO Internal Instruction No. 1" copies of which are available from DESP 3. Such requests are subject to case-by-case consideration through the MOD Form 680 procedure (see para 1155). Companies should be directed to the appropriate RMD for details.

Release overseas of private venture information

1173. Prior to the release of private venture funded information overseas, its protection should be determined in consultation with DD DefSy(S&T). As in the case of Government- owned information, its release is then subject to MOD Form 680 procedure.

References

1174. When documents are being released, care should be taken to avoid references to reports which would not be supplied because of their protective marking or sensitivity.

Security of information concerning sales

1175. Prior to material marked CONFIDENTIAL or above being delivered to an overseas country, a Memorandum of Understanding (MOU) to cover security, intellectual property rights (IPR), claims, etc must be signed between Her Majesty's Government and the recipient Government before delivery starts. However, where a general security MOU exists with the recipient country, for security purposes, reference to this document in the MOU is all that is required.

1176. On occasions there is a need to arrange for the release of information carrying a higher protective marking than equipment to be supplied. When such instances occur, this release must also be the subject of an MOU.

1177. The existence of an MOU is particularly important where UK protected material is being supplied to countries which do not have direct equivalents to our protective markings. The MOU will describe the security protection to be afforded to

material at each level of UK protective marking.

1178. In the absence of a General Security MOU, all other MOUs relating to the sale of protected equipment and the release of associated information must contain security clauses, as required under para 1175 above, and InfoSy(Industry)1 advice is to be sought.

Patent security agreements

1179. Patent action in support of present or eventual commercial exploitation need not necessarily be prevented by military security considerations; the United Kingdom has patent security agreements with a number of countries so that patent applications can be made to cover patentable information even though it may be protected. A patent security agreement between the UK Government and a foreign Government should be made to ensure that information released by one to the other will be afforded the same degree of protection by the receiving Government as it was given by the releasing Government. Under the agreement it is then possible to arrange for patent applications to be made in the security section of each country's Patent Office and to be withheld from publication until the security restrictions are lifted. Patent protection in the conventional sense could not begin until then, but the arrangement does not affect the priority date for the eventual patent.

1180. It is generally part of such a patent security agreement that a country wishing to file a security classified patent application in another country's Patent Office shall also transmit a copy of the information (patent specification) to the other country's defence authorities. More detailed information about these arrangements is available from the Intellectual Property Rights Group (IPRG), which files and prosecutes patent applications, and the Inventions Unit – DD DefSy(S&T), which monitors the implementation of the patent security arrangements.

Courses

1181. Foreign and Commonwealth students may be admitted to UK military courses as arranged by International Defence Training (IDT) staffs or courses arranged by List X firms. If an IDT course is above the limit set for release of information to the particular nation by Table X then the IDT should seek advice from the appropriate single-Service Principal Security Adviser, before a firm offer is extended.

Unsolicited mail

1182. The guidance given in paragraph 1143 should be applied to unsolicited mail whether received from overseas or in the country concerned.

SECTION III

POLICY FOR THE DISCLOSURE BY THE UNITED KINGDOM OF INFORMATION OWNED BY OTHER COUNTRIES AND INTERNATIONAL DEFENCE ORGANISATIONS

Information relating to projects developed jointly with other countries

1183. From time to time an arrangement is reached by the United Kingdom with one or more countries for the joint development of a particular project. The information resulting from such an arrangement becomes "combined" and as such cannot be released without the mutual determination of all countries participating in the project.

Information of other ownership

1184. Apart from the above, military information received from another country is not to be disclosed to a third country without the agreement of the originating country.

Information owned by NATO

1185. The regulations governing the release to non-NATO countries of classified NATO information, including documents carrying a NATO marking, are contained in the Document C-M(55)15(FINAL) 'Security within the North Atlantic Treaty Organisation'; the approval of the NATO Council must be obtained for any such release. Sponsor branches seeking to make releases which need NATO Council consent are to submit applications to the NATO & European Policy Group (NEPG) which will then forward them through the NATO chain of command to the NATO Council seeking release approval. NATO rules permit all member nations to release any NATO unclassified information to non-NATO countries and also any protectively marked information which is entirely of a national (ie UK) origin. In such cases sponsor branches should satisfy themselves that the release would not be against the interests of NATO. As appropriate Principal Security Adviser staff is to be consulted about the machinery of the release. Governments of countries participating in NATO collaborative programmes may release NATO information relating to the programmes to any country only with the consent of their collaborative partners but without NATO Council consent. UK information relating to these programmes which has not been released to NATO remains subject to UK national release regulations.

Information owned by other international Defence organisations (IDOs)

1186. Similar considerations to those set out in para 1185 apply in these cases. However, any proposal to release information belonging to one of the other IDOs to a country not belonging to that IDO, unless the information is of entirely United Kingdom origin, should be referred as appropriate to Principal Security Adviser staff.

SECTION IV

SECURITY ARRANGEMENTS FOR THE RELEASE OF UK PROTECTIVELY MARKED INFORMATION TO COMBINED JOINT TASK FORCES (CJTFS)/COALITION MISSIONS INVOLVING THE UK ARMED FORCES

Introduction

1187. The following guidance is only to be used in the absence of any security information being issued by the relevant CJTF/Coalition mission responsible for the joint operation prior to and shortly following deployment of UK Armed Forces to the area concerned. However the UK Chief J2/senior security advisor should ensure that the guidance issued by the relevant CJTF/Coalition mission fully reflects the context of this Section.

1188. Participation in c CJTF/Coalition mission by the UK MOD presumes that, along with other nations (eg NATO and non-NATO nations), there shall be a release/exchange of protectively marked information required for the conduct of the CJTF/Coalition mission. This information shall principally be to safeguard the forces involved, to assist in the implementation of the operation and also maintain the effectiveness of the mission.

1189. This guidance only sets out additional security requirements for the release/exchange of UK protectively marked information to a CJTF/Coalition mission. Robust rules, to prevent accidental compromise of UK protectively marked information, should be issued by the Chief J2/senior security advisor covering joint operations' rooms, briefing, IT networks, postal and courier systems etc. JSP 440 should be consulted for detailed guidance regarding the physical security, carriage, handling and accounting procedures for UK protectively marked information.

Release of NATO and WEU information

1190. Guidance on the release of NATO and WEU information to a CJTF/Coalition mission, will be issued as and when appropriate by their respective security authorities.

Principles of release

1191. The following principles shall apply:

m. **UK political/military endorsement** - UK political and military endorsement of the CJTF/Coalition mission shall have been obtained and any

legal requirements satisfied **before** UK protectively marked information can be released/exchanged within a CJTF/Coalition mission;

n. **Security agreements/assurances** - Security agreements/assurances must be completed by all parties before UK protectively marked information can be released to a CJTF/Coalition Mission. An example of a Security Assurance is reproduced at Annex D:

o. **Restrictions on release** - The originator shall be the sole authority for deciding the level of protective marking. Unless the originator specifies any detailed release/restriction instructions on the document, it shall be left to the discretion of the UK Contingent Commander, acting on the advice of his Chief J2/senior security advisor, to balance the requirement to protect UK information with the need to safeguard the forces involved, to assist in the implementation of the operation and also maintain the effectiveness of the CJTF/Coalition mission before deciding whether to release the UK information received. Sensitive intelligence material must not be released without the prior approval of the appropriate national authority. Separate instructions will be issued by such an authority for the protection and/or release of their material.

p. All UK protectively marked information released/exchanged shall be disseminated under strict observance of the need-to-know principle and shall only be used for the accomplishment of the CJTF/Coalition mission;

q. **Delegation of release/exchange authority** - During a CJTF/Coalition mission, in order to ensure the safety of forces and the effectiveness of the mission, the UK Contingent Commander may, in consultation with his Chief J2/senior security advisor, and after the issue of appropriate guidelines, delegate authority for the release/exchange of all UK protectively marked information of an urgent operational nature, such as support of combined combat operations, to those UK officers best suited to evaluate the importance of that information and the need for its immediate release. This should be specified in the promulgation of Operations Order. The guiding principle shall be that UK protectively marked information of an urgent operational nature, that has the potential to affect the lives of CJTF/Coalition personnel, should be withheld **only** in the most exceptional circumstances. Consideration may also have to be given to editing the information in such a manner as to protect UK national sources, when necessary.

r. Once established, the security policy and procedures for the handling of protectively marked information, of the lead organisation/nation, shall apply to the UK Armed Forces contingent participating in the CJTF/Coalition mission;

Ownership and protective markings

1192. There may be a requirement to release/disseminate UK protectively marked information for the planning/preparatory stages of the CJTF/Coalition onwards. Originators should, therefore, designate as much UK protectively marked information as possible as releasable to the CJTF/Coalition mission. UK commanders should seek to anticipate requirements for UK protectively marked information at the earliest possible stage and seek approval for its release/dissemination as outlined in paragraph 1194 below. Separate compartments for UK only and for UK protectively marked information released to the CJTF/Coalition mission must be created in order to provide a mechanism to control the circulation of protectively marked information within the CJTF/Coalition mission.

1193. When it is decided that UK information can be released, the ownership, protective marking and lifing of UK information should be clearly identified as follows:

s. **Ownership/protective marking** - All information shall be protectively marked in accordance with the instruction set out in JSP 440 and prefixed "UK";

t. **Release designators** - Each document will carry a release designator, where appropriate, as in the examples below:

(1) **UK SECRET**
Releasable to (Name of CJTF/Coalition mission)

(2) **UK SECRET**
Releasable to (eg WEU/NATO members only/CJTF/Coalition mission

(3) **UK SECRET**
Releasable to (name of CJTF/Coalition mission - Name/Names of Country(ies) only)

u. **Downgrading/destruction** - Wherever possible, the originator should indicate below the protective marking and release details, that the document can be downgraded or destroyed after a certain period of time. Destruction, in most cases, will be preferable to downgrading unless there is a demonstrated need for retention. This should be considered for all UK information which will become generally known after a specific date or event eg. at the end of a mission/operation.

Information Systems

1194. An increasing amount of information is now carried on information systems

such as portable laptop computers. Therefore the UK Contingent Commander, in consultation with the Chief J2/senior security advisor, should appoint an Information Technology Security Officer (ITSO) to ensure that all software and hardware used by the CJTF/Coalition mission is handled and protected in accordance with JSP 440, Volume 3 - Information Technology.

Protectively marking individual paragraphs

1195. Individual paragraphs of UK documents protectively marked CONFIDENTIAL and above, should be protectively marked by the originator to allow further dissemination of appropriate sections. Original protective markings/caveats must be retained when information is used to prepare composite documents or briefings.

UK protectively marked information exclusively for UK Armed Forces

1196. UK protectively marked material for UK Armed Forces use only must be kept totally separate from that of UK information which can be released/disseminated to the CJTF/Coalition mission. There will be a need to provide a separate mechanism to control the circulation of UK protectively marked information within the CJTF/Coalition mission. This will be achieved by:

a. Establishing separate UK facilities for the collation and screening of UK protectively marked information prior to release. These facilities will be at the lowest level consistent with the security and effectiveness of the CJTF/Coalition mission;

b. Permitting access to UK secure areas by non-UK personnel only when escorted;

c. Prohibiting access by non-UK personnel to primary sources of UK protectively marked information or to IT systems and networks processing UK protectively marked information;

d. Permitting access by non-UK personnel to meetings/briefings only after UK protectively marked information to be used in them has been approved for release;

Release authority

1197. These authorities are listed in order (only in respect of UK protectively marked information) as follows:

v. the originator of the document;

w. the UK Contingent Commander, in consultation with his Chief J2/senior security advisor, of the CJTF/Coalition mission; or

x. designated UK officers given delegated authority by the UK Contingent Commander, in consultation with his Chief J2/senior security advisor.

This page intentionally left blank.

ANNEX A TO CHAPTER 11

CONDITIONS OF RELEASE LABELS/STATEMENTS FOR DOCUMENTS RELEASED TO OVERSEAS RECIPIENTS

1. The conditions of release labels/statements described in **paragraphs 4-7** below are to be used by the Ministry of Defence on all protectively marked and unclassified documents which have been approved for release to other named Governments except those unclassified documents which can be given unlimited distribution, or papers for which there are no special handling requirements. The term 'document' should be interpreted widely to not only include formal technical or scientific reports but also technical memoranda, tabulated data, trials, reports etc.

2. Limitation on the release of unclassified information might, for example, be imposed because it contains information the dissemination of which would be prejudicial to proprietary rights, undesirable references to other documents, adverse comment on a contractor's product, or information which, although not of itself worthy of a protective marking has an intelligence value (eg which reveals a field of interest), or, if the sale of equipment would not be allowed, there would be no reason to release any information.

3. Sponsor branches wishing to release documents are to decide which labels/statements will apply for each release. Where copyright in documentary information and/or proprietary rights belong to Her Majesty's Government or a United Kingdom contractor, it is necessary to obtain permission before releasing the document to other governments or their contractors. Further, if information comprises manufacturing drawings, reports, design data, etc arising from work done under a development contract, it should not be assumed without verification that rights in such information are owned by Her Majesty's Government and the advice of Defence branches should be sought. In addition, information marked higher than RESTRICTED should not be released to any Commonwealth or foreign visitors unless the sponsoring authority has obtained confirmation from the appropriate Principal Security Adviser that the visitor has the appropriate security clearance.

4. **LABEL/STATEMENT 'A'** is to be applied to documents which the recipient Government may release to its defence contractors within its own territory. Label/Statement 'A' reads as follows;

"a. This information is released by the United Kingdom Government to the _____ Government for Defence purposes only.

b. This information must be afforded the same degree of protection as that afforded to information of an equivalent classification originated by the

recipient Government or as required by the recipient Government's national security regulations.

c. This information may be disclosed only within the Defence Department of the _____ Government and to its Defence Contractors within its territory, except as otherwise authorised by the UK Ministry of Defence. Such recipients shall be required to accept the information on the same conditions as the _____ Government.

d. This information may be subject to privately owned rights."

5. **LABEL/STATEMENT 'B'** is to be applied to documents which require a special circulation to individuals outside Defence Departments of the recipient Government. Label/Statement 'B' reads as follows:

"a. This information is released by the United Kingdom Government to the _____ Government for Defence purposes only.

b. This information must be afforded the same degree of protection as that afforded to information of an equivalent classification originated by the recipient Government or as required by the recipient Government's national security regulations.

c. This information may be disclosed only within the Defence Departments of the _____ Government and to those noted below, except as authorised by the UK Ministry of Defence. Such recipients shall be required to accept the information on the same conditions as the _____ Government.

d. This information may be subject to privately owned rights.

e. Names and addresses of those authorised to receive this information:

_____"

6. **LABEL/STATEMENT 'C'** is to be applied to documents which the recipient Government may not release to anyone outside its Defence Department. Label/Statement 'C' reads as follows;

"a. This information is released by the United Kingdom Government to the _____ Government for Defence purposes only.

b. This information must be afforded the same degree of protection as that afforded to information of an equivalent classification originated by the recipient Government or as required by the recipient Government's national security regulations.

c. This information may be disclosed only within the Defence Departments of the _____ Government, except as otherwise authorised by the UK Ministry of Defence.

d. This information may be subject to privately owned rights".

7. **LABEL/STATEMENT 'D'** is to be used in conjunction with labels 'A', 'B, or 'C' in those cases where the copyright of the document and proprietary rights belonging to Her Majesty's Government or to a United Kingdom contractor might be prejudiced by its disclosure. It is intended to safeguard these rights and those owned by Departments. The permission of British contractors must be obtained before their documents are released to a foreign Government and its contractors. Label/Statement 'D' reads as follows:

"a. This information is released for information only and is to be treated as disclosed in confidence. The _____ Government is to ensure that this information is not dealt with in any manner likely to prejudice the rights of any owner to obtain patent or other statutory protection therefore.

b. Before any use is made of this information for the purpose of manufacture, the authorisation of the UK Ministry of Defence must be obtained."

8. Other conditions of release may be applied where it is desired to restrict the release of information overseas for special purposes or in special ways. The wording of such conditions should be agreed with the Principal Security Adviser.

This page intentionally left blank.

ANNEX B TO CHAPTER 11

THE SAFEGUARDING OF COMMERCIALLY SIGNIFICANT INFORMATION IN TECHNICAL MEMORANDA AND REPORTS

1. To avoid any misunderstanding regarding the disclosure of commercially sensitive information, documents carrying the descriptor marked COMMERCIAL are to incorporate appropriate instructions to recipients. Companies having proprietary rights to information in such documents must signify their agreement to disclosure before MOD permission for disclosure can be given. Where disclosure of information is to be controlled or otherwise limited, documents are to carry Conditions of Release" instructions (detailed at Paragraph 3) after categorisation as follows:

Category 1	Proprietary information made available to the MOD.
Category 2	MOD information of significant commercial value.
Category 3	Category 2 information made available for exploitation by the Defence Technology Enterprise. Where applicable, Category 3 labels supplement instructions appropriate to Category 2; they should always be applied below a Category 2 label.
Category 4	Relate to MOD originated documents including any sensitive proposal, assessment or statement which should not be released to Industry for reasons other than its potential value as a trade secret.

A document containing information falling into more than one category must bear more than one label.

2. The originator is responsible for categorisation and applying the appropriate label(s). IPRG should be consulted if there is any doubt about the appropriate category or label to use, and must be consulted before any change in the designation.

Conditions of release labels for technical memoranda and reports containing sensitive commercial information

3. The following text must be conspicuously marked on Technical Memoranda and Reports containing Sensitive Commercial Information:

Category 1 Documents

COMMERCIAL 1

RELEASE CONDITION

This document contains proprietary information made available to MOD subject to limitations of confidentiality and restricted rights of use. Its existence or contents must not be disclosed outside MOD without specific authority. Patents Directorate should be consulted if outside use or disclosure is contemplated.

Proprietary Information

Category 2 Documents

COMMERCIAL 2

RELEASE CONDITIONS

This document contains MOD information of significant commercial value. It must not be disclosed outside MOD without specific approval from Patents Directorate which will be given only for disclosures to persons who have signed relevant confidentiality agreements, licence agreements or contracts.

MOD Information

Category 3 Documents (Text to appear following that described for Category 2)

3

DTE Exploitation

Made available for release and exploitation through Defence Technology Enterprises Ltd to UK firms under confidentiality agreements.

Note: This does not affect the right of release by MOD for use on MOD contract work.

Category 4 Documents

4

COMMERCIAL

MOD only

This document and the information it contains are for use within UK Government only and must not be released to any other persons without the agreement of the originator.

ANNEX C TO CHAPTER 11

SECURITY OF OFFICIAL MAPS, CHARTS, PLANS, AIR PHOTOGRAPHS (INCLUDING AIR PHOTO-MOSAICS AND FILMS) AND DIAGRAMS

Maps, charts and plans

1. There are a small number of MOD sensitive establishments and installations (hereinafter referred to as "sensitive sites") which it would not be in the national interest for full details of them to be included on maps, charts and plans that are made available to the public. However, the general public, business and other non-government organisations are entitled to expect that the maps, charts and plans supplied by government are accurate, reliable and comprehensive. Information must not therefore be omitted from such documents unless this is necessary to protect the safety and security of the sensitive site concerned.

2. **Identifying and registering sensitive sites.** It is considered most unlikely that the majority of MOD establishments and installations will be placed at threat by the release of normal, comprehensive survey information unless all the following criteria are met:

a. the establishment or installation is assessed to be at enhanced threat of terrorist attack or other forms of serious crime, or is a potential target for Foreign Intelligence Services;

b. the survey information which the establishment wishes to omit would provide useful information to terrorists, to foreign intelligence organisations, or to others planning serious criminal activities;

c. the survey information to be omitted could not readily be obtained by other means (eg by observation from public access to the site, from the site boundary or from a suitable vantage point, including legitimate oversight or from existing published sources).

d. Each Principal Security Adviser keeps a list of sensitive sites within its area of responsibility. These lists are reviewed annually to consider if there is a continuing need for map, chart, plan or photography restrictions to apply to the sites which have been identified.

e. The integrity and effectiveness of the arrangements for applying these restrictions, depend on keeping the number of sites to a minimum.

f. USyOs or ESyOs concerned about the sensitivity of their sites, in

relation to providing official site survey information, should contact their appropriate Sector security staff for advice.

3. **Landmarks essential for public safety.** The application of the arrangements described above is subject to the need to retain an indication of landmarks considered to be essential to safe navigation by sea or air.

4. The MOD considers itself bound, in the interests of safe navigation, to indicate on its published charts, radio stations which give navigational direction-finding service and certain installations on land which would be conspicuous to a mariner from seawards. Nevertheless, the latter need not be specified in detail, and they are in nay case very prominent objects which cannot be concealed. In addition, overhead cables must be shown where they cross waterways, thereby limiting headroom. The MOD also considers itself bound to show names against marine terminals, jetties, wharves etc connected with sensitive sites where such names are of vital interest to shipping.

Air photographs (including air photo-mosaics and films) and diagrams

5. It is recognised that, except where overflight is prohibited by air traffic regulations, it is impractical to regulate the activity of "taking" aerial photographs and that any control - which in practice is likely to be little more than influence - can only be applied to their sale or distribution. In addition, this approach can only be directed towards the professional aerial photography companies: there is little or no effective control over others who have the ability to take photographs from the air. Only professionals, however, are likely to have the very expensive equipment needed to take high-resolution photographs which themselves pose the greatest threat to security.

6. Guidance to the press and commercial photography companies is given by the Secretary of the Defence, Press and Broadcasting Advisory Committee (DPBAC) as is prescribed in DA Notice No 5 - "Identification of Specific Installations".

7. **Aerial surveys by foreign firms.** An application for a foreign registered aircraft to carry out aerial survey or other similar flights over the United Kingdom would normally be submitted to the Department of Trade, who after appropriate enquiry would submit it for clearance to the Sec/DPBAC. Any application, from whatever source, received directly within the MOD, should be referred to Sec/DPBAC.

Handling material containing information about sensitive sites

8. All official maps, charts and plans which merit security protection should be overstamped with the appropriate protective marking. Protectively marked maps, charts and plans may be issued only to those who have a "need-to-know" and are authorised to receive them; the directorate/unit responsible for the protectively marked content should always be consulted.

9. Official photographs (including air photo air-mosaics and films) and diagrams which include any of the sensitive sites covered by this guidance should be similarly treated.

10. Guidance on the regulation of air imagery from Service sources is contained in JSP 348.

Open Skies

11. This guidance does not apply to photography carried out under the Open Skies Treaty.

This page intentionally left blank.

ANNEX D TO CHAPTER 11

SECURITY ASSURANCE

1. The (country or organisation) represented by (name, rank and function) in the furtherance of the (name of the CJTF/Coalition mission) agrees:

a. to safeguard UK protectively marked information provided to it by the United Kingdom of Great Britain and Northern Ireland in a manner equivalent to that used to protect its own classified information of an equivalent or higher level;

b. to provide such UK protectively marked information only to appropriately cleared individuals under its jurisdiction with a need-to-know;

c. to use the information only for the purposes for which it was provided;

d. not to transfer the information to a third party **without** the prior written approval of the originator of the information; and

e. to abide by any other conditions of release or security requirements conveyed by the Commanding Officer (or his delegated representative) of the UK contingent, even after completion of the (name of the CJTF/Coalition mission).

This page intentionally left blank.

CHAPTER 12
CONTRACTS SECURITY

This page intentionally left blank

CHAPTER 12

SECTION I

CONTRACTS SECURITY

SUB-SECTION IA

INTRODUCTION AND DEFINITIONS

Introduction

12001. This Chapter describes the security procedures which apply and the protective arrangements which need to be implemented in connection with the award of a protected contract to Industry.

12002. The security measures which are necessary depend on the protection given to:

a. the work to be performed on the contract (or subcontract) and

b. the official information to be disclosed to the contractor.

The security measures afforded to any contract, at any level, for goods or services depend on the protective marking of the contract. Before deciding on the protective marking of any contract the security authority of the requisitioning branch or establishment (see below) is to be consulted to ensure that the protective marking proposed by the requisitioning branch or establishment is correct. The security authority should normally be approached before the feasibility study is written, and certainly before the invitation to tender is offered. For protective markings of CONFIDENTIAL or above, the full range of security measures described in this chapter are applicable. Where the marking does not exceed RESTRICTED, the security measures are less stringent and are summarised in Sub-section 1K. Care must be exercised to distinguish between the protection given to the work performed or information disclosed under the contract and the protective marking of the tender or contract documents themselves which are generally lower. (See Sub-section 1D).

Definitions

12003. **Requisitioning branches or establishments.** The term 'Requisitioning branch' (RB) means the technical, supply or project branch which raises the contract action request for the supplies or services in question.

12004. **"Secret Matter" and "Restricted aspects".** The term 'Secret Matter', is any matter connected with or arising out of the execution of a contract marked CONFIDENTIAL or above. The term 'Restricted Aspects' similarly refers to material or aspects of information marked RESTRICTED. The 'Secret Matter' and the 'Restricted Aspects' are defined to the contractor in a 'Security Aspects Letter' (SAL), or by a 'Security Aspects Clause' in the contract, or by a Restricted Aspects Letter.

12005. **Contract Arrangements.** For the purpose of these instructions, the term 'contract' covers invitations to tender, tenders, advance orders, contracts, extracts and orders.

12006. **List X.** This term refers to contractors or subcontractors who have been formally placed on List X because they are undertaking work marked CONFIDENTIAL or above - "On the Company Premises". **Contractors who are on the list are not entitled to any preferential status in the granting of new contracts**.

12007. **"Authorised for Access".** In Industry a personal security clearance allowing access to protected information up to and including SECRET is known as "Authorised for Access".

Security Advisers

12008. **The security authority.** The security authority is the security branch ultimately responsible for identifying and overseeing the security aspects of a contract.

12009. Officers of the Security Service, in their capacity as advisers on security in industry, visit a contractor who has received his first contract marked CONFIDENTIAL or above as soon as possible after the contract has been placed. They advise the contractor on the security measures necessary, including personnel security, which must be taken to safeguard the "secret matter" of the contract in accordance with the obligations imposed by DEFCON 659. Advisers have no powers to visit or advise a contractor until a contract protected at this level has been let. NB The value and scope of this advice will be severely limited until the "secret matter" of the contract has been notified to the contractor.

SUB-SECTION IB

CONDITIONS OF CONTRACTS RELATING TO SECURITY

The two conditions

12010. The following condition relates to security:

DEFCON 659 - Security Measures

In addition, there is a condition covering both protected and UNCLASSIFIED information primarily for protection of intellectual property rights interests:

DEFCON 531 - Disclosure of Information

. The texts of DEFCONs 531 and 659 are reproduced as Annexes A and B.

12011. All Government contracts placed in the UK are subject to DEFCON 531 but where it is necessary to disclose to the contractor information marked CONFIDENTIAL, SECRET, or TOP SECRET, DEFCON 659 must also be included. DEFCON 659 takes precedence over DEFCON 531

12012. DEFCON 659 is not to be used for contracts placed with Overseas contractors. The security provisions for these and other types of contracts are dealt within Sections 8 and 9.

DEFCON 531 (Disclosure of Information)

12013. DEFCON 531 requires the contractor to safeguard information provided by MOD and requires him to ensure his employees are aware of his arrangements for so doing before they receive information. There is a mutual obligation to treat in confidence all information disclosed in connection with or under the contract.

DEFCON 659 (Security measures)

12014. Contracts which involves disclosure of information marked CONFIDENTIAL, SECRET or TOP SECRET are subject to DEFCON 659 which apprises the contractor of the necessary security precautions.

12015. Amongst other things DECON 659 draws attention to the provisions of the Official Secrets Act and obliges the contractor:

a. To allow only persons approved by the Ministry of Defence and with a valid "need to know" to have access to the "secret matter".

b. To safeguard the "secret matter" strictly at all times to the standard prescribed.

c. To ensure that employees with access to the "secret matter" are aware of and observe the security obligations imposed on the contractor and to report any default on their part.

d. Not to place subcontracts involving disclosure of "secret matter" without the Ministry of Defence's written consent, and to include security conditions as defined in Appendix to DEFCON 659.

e. To allow the Ministry of Defence to inspect his security arrangements.

f. To permit no information in any form whatever to be published, or circulated except as necessary for the work, without the Ministry of Defence's written consent.

DEFCON 76 (Conditions applicable to work performed by contractors' personnel at government establishments).

12016. DEFCON 76 is included in contracts where work is performed by contractors at Government establishments. Some of its provisions relate to the control of contractors' employees who require access to protected information or where it would not be possible to exclude them from access to protected information, even if the work upon which they are engaged is UNCLASSIFIED. In such circumstances this condition may be used in conjunction with, but never instead of DEFCON 659. DEFCON 76 is reproduced at Annex C.

DEFCON 76 also obligates the contractors employees to comply with any rules, regulations and requirements in force whilst at the establishment as required and dictated by the Head of Establishment or his delegated official. For security, the applicable requirements of JSP 440 will be required to be communicated to the contractors personnel and overseen by the Establishment Security Officer (ESyO). In addition, and where appropriate, PPP/PFI/CFQ Guides and the provisions of the Template of Security
Requirements at Annex X may also be applied**.**

SUB-SECTION IC

RELEASE OF PROTECTIVELY MARKED INFORMATION TO INDUSTRY

Rules governing the release of information marked CONFIDENTIAL or above to UK contractors.

12017. A contract which is subject to DEFCON 659 may be placed only with companies who have been approved by Info Sy (Industry)2/3 to undertake work marked CONFIDENTIAL or above at a specified location or address. With the exception of preliminary negotiations of a general nature, as provided for in para 12018, the Requisitioning Branch, (or Contracts Staff, in respect of any company it wishes to add to the list of those to be invited to tender as recommended by the Requisitioning Branch), must obtain approval from Info Sy (Industry)2/3 using the proforma at Annex D, before entering into any discussion, negotiations or the issuing of any invitation to tender that may lead to a contract marked CONFIDENTIAL or above. This applies whether or not it is necessary to disclose any information marked CONFIDENTIAL or above before the contract is placed. **A contractor or his representative may not be told, even informally, that the company, is being subjected to a security check, or that the placing of a contract is subject to security approval.**

12018. Preliminary negotiations of a general nature with the potential contractor may be made prior to approval, provided that:

a. no information marked CONFIDENTIAL or above is disclosed;

b. no indication is given that information marked CONFIDENTIAL or above will be involved in the contract:

c. no commitment is entered into;

d. it is understood that discussions may be terminated without explanation.

12019. Submission to Info Sy (Industry)2/3 for approval may be waived only if the Requisitioning Branch or Contracts Staff (as appropriate) holds unexpired Info Sy (Industry)2/3 provisional approval to release protected matter at the appropriate level to the company.

12020. Officers of the Ministry of Defence must not disclose information marked CONFIDENTIAL or above to a member of a company, however senior, without first satisfying themselves that he has a 'need to know' and has been 'Authorised for Access' to protected information at the appropriate level.

12021. For contractors not on List X Info Sy (Industry)2/3 are responsible for processing "Authority for Access" for the 2 or 3 initial contacts. If the contractor is on List X, the Security Officer, (whose name can be obtained from Info Sy (Industry)2/3) should be asked whether an individual has been "Authorised for Access" to protected information.

12022. When the proposed contractor is on List X or approval by Info Sy (Industry)2/3 has been given to use the company, any disclosure of information marked **CONFIDENTIAL** or above during preliminary negotiations and discussions must be accompanied by warnings that the information is entrusted in strict confidence, that it is protected by, and its recipients are subject to the Official Secrets Act, and that it may be communicated only to other members of the company who have been "Authorised for Access" to protected information by the Ministry of Defence. If protected information is disclosed orally, its protective marking must be made quite clear.

Procedure for obtaining security approval to use a company

12023. Provisional approval. Provisional approval means that there is no objection in principle to a contract marked CONFIDENTIAL or above being placed with the company, but it does not constitute approval of the main body of the contractor's employees, nor that its premises are necessarily suitable for the performance of contracts protected at this level.

12024. **Applications for provisional approval.** When having followed the procedure set out in para 12017, the proforma as at Annex H, is returned by Info Sy (Industry)2/3 indicating in column 'c' that no clearance (whether full or provisional) exists, an application for Provisional Approval should be submitted in writing to Info Sy (Industry)2/3 by the Requisitioning Branch or Contracts Staff (as appropriate) and should include the following:

a. Full name, registered address and company registration number of contractor along with first point of contact.

b. Proposed place of manufacture.

c. Brief description of proposed work.

d. Highest protective marking of information and any special type of information (eg ATOMIC, Caveat) likely to be disclosed in preliminary negotiations and under any eventual contract.

e. Name of employees of the contractor (usually no more than 3) who will require access to information marked CONFIDENTIAL or above at the provisional approval stage.

12025. It is up to the Requisitioning Branch to establish whether the contractor holds the

required QA certification. If the contractor is not qualified, the advice of MOD Commercial Policy Branch should be sought before seeking Provisional Security Approval. Enquiries concerning the company will normally take ten to twelve weeks to complete

If approval is refused by Info Sy (Industry)2/3 the Requisitioning Branch or Contracts Staff must refrain from entering into negotiations with the contractor and must discontinue any exploratory discussions without revealing that security is the reason.

Completion of Security Questionnaire/Supplement

12025. As soon as an application for Provisional Approval is made to Info Sy (Industry)2/3 they will write to the nominated contacts at the company along the lines of Annex I, asking them

to complete the appropriate Security Questionnaires.

Action following provisional approval

12026. Until the award of a protected contract ie at the tender stage, it is the responsibility of the Requisitioning Branch or Contracts Staff (as appropriate) to ensure that any protected information at CONFIDENTIAL level or above released to the contractor is properly protected. The following action must therefore be taken by the Requisitioning Branch or Contracts Staff when passing CONFIDENTIAL or above information to contractors with Provisional Security Approval:

a. Protected documents passed to the contractor must be addressed to a person known to be authorised for access to such information.

b. The contractor must be notified that their premises will be a prohibited place to which the official Secrets Acts 1911-1989 will apply; that the information is entrusted in strict confidence; and that it may be communicated only to other members of the company who have been authorised for access to protected information by the Ministry of Defence.

c. The contractor must be given a copy of the "Memorandum on Security for Contractors", copies of which will be provided by Info Sy (Industry)2/3 with the approval letter.

d. Enquiries must be made to see whether there is likely to be any difficulty about the provision of adequate physical security precautions at the contractor's premises at which the protected work is to be done; for example, whether it would be possible to segregate protected work from other work on the premises. There is, however, no need to go into too much detail at this stage. If a contract is placed, a Security Adviser will be appointed and the company placed on list X. However, if the provision of security precautions is likely to affect

programme costs, the contractor must be made aware of the likely requirements at this stage.

e. If at a tender stage protectively marked information at SECRET level is to be sent to the company, the SECRET matter must be copied IMMEDIATELY to Info Sy (Industry)2/3 to allow for arrangements to be made for a security adviser to be temporarily appointed to the company to provide advice on the safeguarding of SECRET material.

f. Those members of the company who will have access to protected information must be asked to sign the Official Secrets Acts declaration form (MOD Form 134) in duplicate; (supplies of which are obtainable from MOD Stores Llangennech). One copy should be retained by the individual and the other returned to the Requisitioning Branch or Contracts Staff (as appropriate) (an example letter is at Annex F).

12027. Where work on a contract marked CONFIDENTIAL or above will be carried out solely at MOD Establishments and there is no need for protected information to be held on the premises of a company, advice and security supervision of the contract, including the arrangements for seeking personnel security approval, will rest with the Security Officer of the Establishment; or if there is no Establishment Security Officer, with the responsible MOD Security Directorate.

Document security

12028. All information marked CONFIDENTIAL or above being despatched to contractors must be sent initially to the Security Officer in the case of a company already on List X; or to the initial contact of the company who will ensure that the information is properly recorded and protected. However, care should be taken to address the Security Officer by name only, not by appointment. **The outside envelope must not bear the words "Security Officer"**. The name of the Security Officer may be obtained from Info Sy (Industry)2/3.

Doubtful marking of documents

12029. A special proforma (copy at Annex M) has been devised for contractors to send to the originators of a protected document, whenever they wish to query the protective marking of any aspect of a contract. Contractors have been assured that the use of these forms will in no way prejudice their interests vis-a-vis Government Contracting Departments. An officer of the Ministry of Defence receiving one of these forms should deal with it promptly, if necessary issuing an amendment to the SAL, which should be distributed in accordance with para 12055.

Visits to contractors

12030. Under clause 3 d) of DEFCON 659, a contractor has a duty to ensure that a visitor has written approval from the Ministry of Defence to discuss protected matters. He also has a duty to satisfy himself about the 'need to know' of any visitor, whatever his status. This latter requirement applies equally to RESTRICTED and UNCLASSIFIED matters.

12031. In order to avoid delay and embarrassment at the time of a visit, officers of the Ministry of Defence should observe the following rules:

a. When intending to visit a contractor for the first time, they should ensure that they are introduced beforehand by letter from the Head of Branch or some other officer known to the contractor. The letter should be sent to the contractor's Security Officer.

b. They should give adequate warning of all subsequent visits.

c. They should not take persons unknown to the contractor on a visit without giving prior warning, and without notifying the contractor of the names of the individuals and the degree of access required.

d. If sponsoring unaccompanied visitors, they should give advance notification together with personal details, confirmation of 'need to know', and degree of access required.

e. They should not seek to use their official position to try to convince a contractor of their 'right' to have access to protected information connected with contractors or to visit parts of his premises other than those with which they are personally concerned.

Visits from contractors

12032. An officer who is to receive a visitor from a company must determine whether he may be given protected information. The contractor must not be allowed to acquire protected information nor is he to be given it, unless he needs to know it and has been authorised to receive it (see paras 12020 and 12021). Disclosure of information marked CONFIDENTIAL and above must first be authorised by the Security Directorate or local security officer.

12033. The person visiting should be escorted at all times **unless** that person satisfies the required security status for unescorted access (see para 12033 above). He must be left in no doubt about the protective marking of any information that has been disclosed to him and then he is responsible for safeguarding it (see para 12022). If documents marked CONFIDENTIAL or above are handed out at demonstrations, conferences etc, each document is to be copy numbered and strictly controlled, and the names of persons

receiving copies recorded. At the end of each session of the demonstration, conference etc, visitors are to hand in their copies. When transmission is to be made to their official address, this must be done through normal secure channels. However, the material should be addressed initially to the security officer of the company (see para 12029) who will ensure that the documents are properly recorded and safeguarded. Further guidance on control and transmission of protected documents is given in Chapter 4.

Recovery of documents etc

12034. Clause 4b) of DEFCON 659 gives the Ministry of Defence the right, by giving notice, to require the contractor to deliver to the Ministry of Defence any document (including all copies and extracts therefrom) which contain or may reveal information about any "secret matters". Requisitioning Branches must ensure that protectively marked documents etc are withdrawn from the contractor on completion of the contract, unless they need to be retained for a further contract, or as inspection records for a certain period. Similarly all branches which have issued protectively marked documents or drawings to contractors in connection with an invitation to tender should ensure that such documents and drawings are recovered from all but the successful tenderer immediately the result is known.

SUB-SECTION ID

PROTECTIVE MARKING OF WORK AND DOCUMENTS

The responsibility of the requisitioning branch

12035. It is the responsibility of the Requisitioning Branch when submitting a requisition or other request for tendering or contract action to answer the following questions in the space provided on the Requisition Form:

a. Will the execution of this contract involve the disclosure and/or custody of information marked CONFIDENTIAL or above on the contractors premises?

b. What is the highest protective marking of information to be included in the tender or initial contract documents?

If disclosure of protected information is solely on MOD premises, an affirmative answer should still be given to the question in para 12038a, but the requisition form must be annotated with a request for DEFCON 76 to be included in the tender or contract document (see para 12016).

12036. If the answer to the question in para 12036a is that information marked CONFIDENTIAL or above will be disclosed, the Requisitioning Branch must take action in accordance with Sub-section IC. In addition, the Contracts Staff must include DEFCON 659 in the tender or contract document.

Protective marking of contract documents

12037. When considering para 12036b, Requisitioning Branches should bear in mind that contract documents have a wide circulation in companies, and the aim should therefore be to exclude information marked CONFIDENTIAL or above from contract documents. If it is not possible to avoid protectively marking the contract document itself, the Requisitioning Branch should consider whether the particulars which will need to appear on the advice, inspection note and on bill forms can be couched in UNCLASSIFIED terms. **Reference to "vetting", "security clearance" of the company must not appear in contract documents** (see paragraph 12017). All contracts subject to DEFCON 659 must bear a protective marking no lower than RESTRICTED.

MOD Contracts Bulletin

12038. When compiling entries for the MOD Contracts bulletin, Requisitioning or

Contract Branches must ensure that each entry is UNCLASSIFIED. It is also essential to ensure that the subscriber will not be able to build up a picture of a protected project from the scanning of a number of UNCLASSIFIED entries. Requisitioning Branches must therefore consult the Project Branch and the Operational Requirements Branch before forwarding entries for inclusion in the bulletin, which relate to a protected contract.

European Journal

12039. Depending upon the value of a particular contract, EEC legislation requires that such contracts must also be advertised in the European Journal. However, where a contract will involve access to protectively marked information bearing a national caveat, or will involve access to sensitive sites/equipment, an application for exemption to advertise should be submitted for Info Sy (Industry)1 for consideration.

SUB-SECTION IE

SECURITY ASPECTS LETTERS

Notification of "SECRET MATTER" to the contractor

12040. The "SECRET matter" in an invitation to tender (ITT), or contract containing DEFCON 659 must be defined to the contractor in writing. The special obligations laid upon the contractor become legally effective only when the Ministry of Defence has issued a notice, in writing, defining which aspects of the ITT or contract are to be marked as CONFIDENTIAL, SECRET, or TOP SECRET. This is achieved by means of a Security Aspects Letter (SAL) written by the Requisitioning Branch, or by the inclusion of a Security Aspects Clause in the ITT or contract. The contractor is required to confirm in writing that he understands and will implement the provisions of the SAL or clause. The SAL must therefore be issued to the contractor along with the ITT or contract document. Info Sy (Industry)2/3 must be informed in advance if this is not possible. It is sometimes unnecessary to define the "secret matter" to the contractor in the form of an SAL. This is usually the case when all access to protected information will be on a Government property only – eg. the employment of consultants etc. In these circumstances, the Requisitioning Branch should include of the following clause in the contract, under security measures:

> "The requirement under DEFCON 659 for the provision of a Security Aspects Letter is waived, as all work on the contract will be carried out on Government premises only."

Advice on the compilation of SALs can be sought from Def Sy (S&T). Any difficulties which the company foresees or experiences in protecting the "secret matter" should be referred to Info Sy (Industry)2/3.

Importance of defining "SECRET matter" to the contractor

12041. The importance of defining "SECRET matter to the contractor are explained as follows:

a. The aim of the SAL or security aspects clause at the tender stage is to ensure that the contractor safeguards protected information, documents or material adequately during and after the tender stage; and to enable the contractor to make financial provision in the tender for the measures which will need to be taken to safeguard the "secret matter" in the event of them being subsequently awarded the contract.

b. The aim of the SAL or clause in the contract is to provide guidance on the security markings of the main features of a project and those sub-assemblies

or components from which any of the protected features might be deduced.

12042. Contracts Staff will be guided by SALs when protectively marking their correspondence and it is therefore important that all sensitive features of the work which are likely to be the subject of correspondence between Contracts Staff and contractors should be correctly identified.

Points to be considered by requisitioning branches in the preparation of a SAL

12043. Points to be considered by the Requisitioning Branch in preparation of a SAL are:

a. A SAL which gives only provisional guidance must be amplified by the Requisitioning Branch directly with the contractor as soon as possible. When a contract is placed following consideration of tenders, a further SAL, as set out in para 12049 below, must be issued by the Requisitioning Branch even if there is no change in the definition and passed to the Contracts Branch.

b. Separate notification of "secret matter" must be made for each new contract; it is **not** sufficient to state that these are the same as for previous contracts even though it maybe the continuation of an on going task.

c. When the work to be undertaken by the contractor does not stem from a Service requirement (eg research initiated by the Ministry of Defence), the appropriate protective markings may have to be decided by the R&D establishment or project branch concerned, in consultation with Def Sy (S&T) in the first instance.

d. When production is current with, or follows research and development, the project branch which acts as Requisitioning Branch must consult the appropriate HQ R&D branch to ensure that the definition of "SECRET matter" is consistent with that given at the research and development stage.

e. Projects at very early stages of development may not yet have been considered by a technical grading committee; it is then necessary to seek the advice of the OR Branch sponsoring the project and Def Sy (S&T). The Requisitioning Branch together with the sponsor and Def Sy (S&T) should then analyze the project, and allocate appropriate protective markings to the main features, assemblies and sub-assemblies which need to be protected, in a Technical Grading Guide if necessary.

f. Project and technical branches should consult the appropriate technical grading authority when in doubt about the definition of "secret matter" aspects in relation to defence equipment.

g. SALs should be protected strictly according to content, and care should be taken not to overgrade them. For instance, if certain aspects of an equipment, such as the weight or internal dimensions, are SECRET, then the letter should simply state that fact, without giving any actual figures. The SAL may then be protectively marked no higher than RESTRICTED.

h. In running contracts which cover both protected and UNCLASSIFIED work, eg contracts for drawing, reproduction or film processing, it will be sufficient for the "secret matter" to be defined in general terms such as any [drawing etc] marked CONFIDENTIAL, SECRET or TOP SECRET.

i. The association of one piece of equipment with another, or of one component part with one or more other parts (the several parts having perhaps been manufactured by different contractors) may require protection. In some cases, the fact that an UNCLASSIFIED, proprietary component is being used in an item of equipment may require protection; in such cases the "association" of the component with the equipment must be protected.

j. The use of blanket technical protective markings must be avoided.

k. The contractor must be notified of the protected aspects of any equipment issued to him on embodiment loan.

l. In certain sensitive fields of work, it may be necessary to protect knowledge of the destination of equipment and to give detailed instructions on security during transportation and storage. If a Technical Grading Guide is issued, these details must be included.

m. It may be necessary to protect the numbers on order and/or the delivery programme and costs.

n. It may be necessary to protect the "existence" of the project.

Level of signature

12044. It is important that SALs should be signed at such a level as to reflect their importance. It is not possible to lay down hard and fast rules, but as a general rule, the signatory should not be less than Band C1. The signatory should also be competent to answer technical questions on matters of detail arising from the definition of the "secret matter". Where this is not possible (eg when the Requisitioning Branch is acting on behalf of an outstation establishment) the name and telephone number of the individual to whom detailed technical enquiries should be referred to should be included in the SAL.

Example letters

12045. Examples of the type of Security Aspects Letters are reproduced at Annexes G to L.

a. Annex G is for tenders to UK List X contractors.

b. Annex H is for tenders to UK contractors with "Provisional Approval" (see Section 3).

c. Annex I is for tenders to UK contractors with Provisional Approval and where RESTRICTED information only needs to be released at the tender stage (see Chapter 3)

d. Annex J is for contracts to UK List X contractors.

e. Annex K is for contracts to UK contractors with "Provisional Approval".

f. Annex L is for a change or amendment to d or e above.

12046. Annexes G - L may be reproduced locally, but there is no obligation to use them provided the content of the appropriate proforma is included in the SAL.

12047. The SAL (undated) must be forwarded to the Contracts Staff with the requisition or request for tender action. Any contract proposal for protected work received without a draft SAL should be returned to the originating branch for further action.

12048. On receipt of a copy of the invitation to tender or contract, the Requisitioning Branch must check that an SAL has been issued, or that the security aspects clause has been included (see para 12054).

12049. The Requisitioning Branch should ensure that a prompt response to the SAL is received from the contractor stating that he understands and will implement the provisions of the SAL.

Use of Technical Grading Guides in SALs

12050. Reference to a Technical Grading Guide simplifies the work of defining the "SECRET matter" to the contractor.

Security Aspects Clause

12051. In those cases where a contractor is already on List X, and when the "secret matter" of a tender or contract can be adequately defined by reference to a Technical

Grading Guide, the Requisitioning Branch may, instead of issuing a separate SAL request the inclusion of the following clause in the tender or contract document, supplying the references to be inserted:

> Security Aspects
>
> For the purpose of DEFCON 659, the "secret matter" of the Contract shall be as defined in ..... The Contractor shall confirm in writing to [the Requisitioning Branch) that this definition of the "secret matter" has been brought to the attention of the person directly responsible for the security of the Contract, that the definition is understood, and that measures can and will be taken to safeguard the "secret matter", and shall immediately refer any difficulty in these respects to [the Requisitioning Branch].

12052. A request to include a Security Aspects Clause **must** be forwarded to the Contracts Staff no later than the Requisition.

Distribution of tenders, contracts and Security Aspects Letters (SALs)

12053. When ITT are issued, the contracts despatch centre (or Contracts Staff in the case of branches which undertake their own distribution) must send the SAL to the Security Officer or main contact in the case of provisional clearance at each firm invited to tender. Similarly, if the Requisitioning Branch has requested the inclusion of a security aspects clause, an extra copy of the tender document only must be sent to the Security Officer or nominated contact. (See para 12029).

12054. Apart from their normal distribution, contracts dispatch centres and Contracts Staff must arrange distribution of copies of the SAL (indicating if it is provisional) with the related contract, to:

a.	Info Sy (Industry)2/3	-	1 copy
b.	Def Sy (S&T)	-	1 copy
c.	Inspectorate of QA Branch	-	1 copy
d.	Outstation establishment	-	2 copies, one to the department concerned with the work and the other to the establishment's security officer.

This page intentionally left blank.

SUB-SECTION IF

AMENDMENTS TO CONTRACTS AND SALS

Amendments to contracts

12055. Amendments to contracts must be protected according to their content, and branches initiating contract amendment action must inform the Contracts Staff of the appropriate protective marking. They must also consider whether the amendments necessitate any alteration or addition to the definition of "secret matter".

Amendment of Security Aspects Letter (SAL) or Security Aspects Clause

12056. When alterations to gradings approved by the appropriate technical grading authority involve amendment to the "SECRET matter" of the contract the Requisitioning Branch must immediately inform the contractor by amending the SAL. The amendment should take the form of Annex L and should be prepared, signed and issued by the Requisitioning Branch.

12057. When the "SECRET matter" is defined by a clause in the contract, and the description in the Technical Grading Guide is changed, the Requisitioning Branch should request the Contracts Staff to make an amendment to the contract in the form of the security aspects clause at para 12054 (adapted to suit the circumstances). The Requisitioning Branch must in the meantime ensure that the contractor is immediately made aware of the changes to the Technical Grading Guide.

12058. Distribution of the amended SAL or contract amendment, should be in accordance with paras 12055 and include the Contracts Staff if appropriate.

Review and amendment of grading

12059. Requisitioning Branches must keep under review the protective marking of all aspects of the contract for which they are responsible. SALs should be reviewed regularly and at least every six months; this regular review, however, must never become a substitute for action as and when it is required (eg by revised protective markings promulgated by the technical grading authority, or by bringing changes to a Technical Grading Guide promptly to the contractor's notice). When changes in design are made, branches should consider and advise the technical grading authority of the possible security implications of the changes.

This page intentionally left blank.

SUB-SECTION IG

SUBCONTRACTS PROTECTIVELY MARKED CONFIDENTIAL OR ABOVE

Approval to place a subcontract protectively marked CONFIDENTIAL or above

12060. Clause 7 a) of DEFCON 659 requires a contractor to seek the Ministry of Defence's approval before subcontracting any work which involves the disclosure of any of the "SECRET matter" of the main contract. This approval is not necessarily required when the place of manufacture of the prospective subcontractor is known to the main contractor to be on List X and contracts subject to DEFCON 659 can, if authorised by the Requisitioning Branch, contain the following provision:

> "Submissions for approval under Clause 7 a) of DEFCON 659 are not required in respect of work to be carried out by subcontractors at premises which are known to be on List X. In other cases the information required under DEFCON 659, Clause 7a) shall be submitted to Info Sy (Industry)2/3 and copied to your Security Adviser in accordance with arrangements notified in "Manual of Protective Security" (MPS).

12061. If a main contractor wishes to place a subcontract involving the disclosure of information marked CONFIDENTIAL or above, on a company not on List X, Info Sy (Industry)2/3 will make an assessment of the suitability of the potential subcontractor solely from a security viewpoint and if there are no objections will notify the main contractor accordingly.

12062. In all cases, the main contractor will be required to include the conditions in the subcontract equivalent as laid down at Appendix to DEFCON 659 and to define to the subcontractor the "Secret Matter" of the subcontract.

Responsibilities of the requisitioning branch

12063. Requisitioning Branches control of subcontracting is based on details provided by contractors when submitting tenders or accepting contracts, and by close liaison with contractors, particularly under Research and Development contracts. Requisitioning Branches should accordingly maintain sufficient liaison with main contractors as will enable them to exercise supervision over subcontracting generally, and to ensure that no more protected information than is necessary is disclosed to subcontractors.

This page intentionally left blank.

SUB-SECTION IH

PROTECTIVELY MARKED CONTRACTS WITH OVERSEAS CONTRACTORS

Application for approval

12064. If it is considered necessary for a contract marked CONFIDENTIAL or above to be placed with a contractor in another country, Ministry of Defence agreement must be obtained in accordance with Chapter 11. The Requisitioning Branch (or the Contracts Staff in respect of any companies it wishes to add to the list of those invited to tender as recommended by the Requisitioning Branch) must then obtain security approval from Info Sy (Industry)1 using the proforma at Annex N before the issue of any ITT or contract or before the release of any information marked CONFIDENTIAL or above; this action must be taken even if the Requisitioning Branch knows the prospective contractor is performing other protectively marked work, or if the contract is to be placed by an authority in the other country on behalf of the MOD (eg the UK Defence Procurement Office in Washington).

12065. The Requisitioning Branch or Contracts Staff (as appropriate) must give Info Sy (Industry)1 a minimum of 10 days notice when seeking security approval of contractors in NATO countries and a minimum of 15 days notice for contractors in non-NATO countries. On no account should CONFIDENTIAL information be passed to an overseas contractor without consulting Info Sy (Industry)1, who will confirm in writing their approval to use the contractor, and provide the appropriate overseas security conditions to be included in the ITT or contract documents. Where a contractor is not already security cleared, advice should be sought from Info Sy (Industry)1, telephone No. 020 7218 4263/0125.

Obligations of an overseas contractor

12066. If Info Sy (Industry)1 gives security approval, the overseas contractor must be provided with details of the information which is protectively marked, and notified that he is required to give at least the same protection to this information as he is obliged to give to information of equivalent security grading entrusted to him by his own government. The Requisitioning branch must prepare an SAL which should be attached to the formal ITT contract documents that are sent to the contractor (see annexes O and P).

Contracts involving the disclosure of RESTRICTED information

12067. There is no requirement to seek security approval from Info Sy (Industry)1

before placing a RESTRICTED contract with an overseas contractor (but see para 12070). The Requisitioning Branch must verify by reference to the instructions on the release of military information (promulgated by the RMIPC) that the country is not one which is debarred from receiving any protected information. The Security Conditions to be included in RESTRICTED ITT or contract documents are reproduced at Annex Q.

12068. The Requisitioning Branch must inform the contractor in writing of the **RESTRICTED** Security Aspects and notify him that this information may be disclosed only to those of his employees who have a "need to know" for the performance of the contract.

12069. Requisitioning Branch or Contracts Staff (as appropriate) should consult Info Sy (Industry)1 using the proforma at Annex N should they wish to place a RESTRICTED contract with a contractor in Australia, Austria, Israel, Italy, South Africa, South Korea, Spain, Sweden, Switzerland, The Netherlands or USA.

Notification of contracts to Info Sy (Industry) 1

12070. One copy of all protectively marked contracts and the SAL, or equivalent, must be sent to Info Sy (Industry)1, one copy of the SAL, or equivalent, must be sent to Def Sy (S&T). Where necessary, Info Sy (Industry)1 will inform the government of the other country, and in the case of contracts involving information marked CONFIDENTIAL or above, will endeavour to arrange for an appropriate department of the other government to accept responsibility of supervising the protection of protectively marked information which will need to be disclosed, as well as the general security of the contract.

SUB-SECTION IJ

OTHER FORMS OF CONTRACTS

Orders on agency establishments or agency factories

12071. For security purposes, contractors managing Ministry of Defence owned establishments under agency agreements are to be treated generally in the same way as other contractors. Certain modification of detailed procedure are, however, necessary on account of the nature of the contractual relationship.

12072. The standing instructions relating to agency establishments include provisions equivalent to those of DEFCON 659. Orders placed on agency establishments which involve access to information marked CONFIDENTIAL or above must draw attention to the relevant security provisions of the agency agreement and the associated standing instructions. Contracts Staff must follow the instructions in para 12055 in despatching an extra copy of an order to the security officer of the agency establishment and in distributing one copy of the order to Info Sy (Industry) 2/3.

12073. An SAL must be issued for each order involving access to information marked CONFIDENTIAL or above. It should take the general form of Annex H, but the reference in the first paragraph should be to sub-paragraph A 1(a) of Section 1 of the 'Standing Instructions Relating to Agency Establishments'. Distribution must be as in para 12057.

Extramural research agreements and consultancy contracts

12074. The majority of research agreements and consultancy contracts are placed with universities or university personnel. Because of the practical difficulties of safeguarding protected information in such circumstances and the universities' own reluctance to handle such information, agreements which involve the disclosure of information protectively marked CONFIDENTIAL or above should only be placed in very exceptional circumstances. DVA(York) should be advised at the earliest possible stage of the intention to place such an agreement.

12075. Before negotiating the agreement, the branch sponsoring it must obtain personal details on Security Questionnaire & Supplement forms (available from the usual forms supplier) of any person who will be engaged in the research, and submit them to DVA(York) for approval. The formal agreement/contract must include a security clause, and Info Sy (Industry)2/3 must be consulted about the wording at an early stage. In general, the security clause will state the protection which must be afforded to the work, and will require, amongst other things, that no person shall be engaged upon the work without the prior approval of the Ministry of Defence, that persons engaged on the

work shall be subject to and sign the Official Secrets Acts declarations, and that protected material shall be protected in accordance with security instructions. A copy of the formal agreement/contract should be sent to Info Sy (Industry)2/3. It is especially important that sponsoring and other branches, who may be asked to approve the engagement of individuals for the work or to agree to individuals having access, should consult DVA(York) before replying.

12076. The personnel working on the agreement/contract will be visited by a Security Adviser who will provide a briefing on their security responsibilities and arrange provision of adequate security furniture. (See also chapters 2 and 5.)

Contracts for buildings and civil engineering works

12077. Some contracts subject to the General Conditions of Government Contracts for Building and Civil Engineering Works (Forms GC/WORKS/1 and CCC/WORKS, C1001 and 2) and to MOD DEFCONS derived there from are placed by the Defence Procurement Agency. These include a 'secrecy' clause drawing attention to the Official Secrets Act and a clause empowering the Ministry of Defence to exclude persons from the site of the work.

Printing contracts placed by MOD with commercial firms

12078. Central Services (Printing) (CS(Pr)) is responsible for the provision of all MOD printing requirements. When a print requirement is identified, MOD Form 1185 for general printing or MOD Form 185a for letter headed paper etc. should be completed and forwarded to CS(Pr)1a. A decision will then be made to either print in-house or through The Stationary Office (TSO) in which case CS(Pr)1 will ensure the work is placed with a contractor who has been approved by Info Sy (Industry) to undertake Protectively Marked contracts.

Local purchase orders

12079. There are no special security provisions in the Conditions of Local Purchase Orders (LPO). It is therefore undesirable for work protectively marked CONFIDENTIAL or above to be placed in this way. Work so marked should be placed by headquarters Contracts Staff responsible for the stores concerned, and if the requirement is recurrent, an enabling arrangement should be considered.

12080. There may, however, be exceptional occasions when it is essential to place a LPO for protected work marked CONFIDENTIAL or above, and in these circumstances it will be necessary to include the full text of DEFCON 659 in the contract (see annex B). LPO work involving protected work CONFIDENTIAL or above may not be placed without the written prior agreement of Info Sy (Industry)2/3.

12081. Local purchase orders must not be placed for film if the purchase price includes

processing, unless it is quite certain that no protected material will be included in the exposed film. Enabling arrangements with the major makers of photographic film contain DEFCON 659 and provide for the direct demand by outstation establishments for supplies of film and for processing where relevant. Special arrangements are promulgated by the contracts division for the handling of protected film under these contracts, and outstation establishments must ensure that these are adhered to when despatching exposed protected film. Any difficulty should be referred to the appropriate Contracts Staff.

12082. The full text of DEFCON 76 should be invoked in RESTRICTED and UNCLASSIFIED LPO where work is performed by contractors' employees at Government establishments (see Annex C).

Contracts associated with international collaborative projects

12083. These may involve special procedures, and if in doubt, Requisitioning Branches should consult Info Sy (Industry)1 and Def Sy (S&T). Bilateral or multilateral collaborative projects are normally covered by government Memoranda of Understanding (MOU), the security clauses of which would normally require a Project Security Instruction (PSI) to be drawn up by the designated project offices in collaboration with the National Security Authorities (NSA)/Designated Security Authorities (DSA) of the participants concerned, as early as is sensible in the life of the project. However, the existence of a PSI does not preclude SALs for individual contracts.

This page intentionally left blank.

SUB-SECTION IK

CONTRACTS INVOLVING THE RELEASE OF RESTRICTED INFORMATION ONLY, TO UK CONTRACTORS

Security measures

12084. Contracts involving the release of information which is marked RESTRICTED should not include DEFCON 659. However, DEFCON 531 (which is applicable where release of UNCLASSIFIED as well as protected information is involved) should be included. The security precautions necessary for the protection of CONFIDENTIAL or above information do not apply to RESTRICTED information. However, such information must only be released on a personal basis to a named UK National in the company and where the contractor is not on List X, Annex R should be included in the Technical Specification or Statement of Work. This gives the contractor advice on the protection of RESTRICTED information.

Notification to the firm of RESTRICTED aspects

12085. The Requisitioning Branch should prepare and sign a RESTRICTED aspects letter to the firm defining the RESTRICTED aspects in the form of Annex S leaving blank spaces for insertion of the ITT or contract number and date. The Requisitioning Branch should forward the RESTRICTED aspects letter to the Contracts Staff with the requisition so that it can be issued with the ITT or contract. If the guidance given is provisional, the Requisitioning Branch should prepare and distribute a further RESTRICTED aspects letter, as soon as possible.

Distribution of RESTRICTED contract/tender documents and SALs

12086. The Contracts Stafff, or contracts despatch centre, should send the RESTRICTED Aspects Letter (RAL), together with the appropriate ITT or contracts document, to the main contact at the company. Copies of the RESTRICTED aspects letter and ITT or contract documentation should be sent to the branches listed in para 12055. When the contractor is on List X a further copy of the RAL and ITT or contract documentation should be sent to the Security Controller.

This page intentionally left blank.

SUB-SECTION IL

SECURITY OF CONTRACTORS' COMPUTER INSTALLATIONS

12087. When processing protectively marked information, the same security policy guidelines apply to computer and information technology systems owned by contractors or subcontractors as for such systems in HMG service. These guidelines are described in the Manual of Protective Security (MPS); Chapter 5 Annex 3 gives the **minimum mandatory** computer security standards for **any** information technology system handling HMG protectively marked information (CESG Compusec Memorandum No 10). DMS Volume 3 reflects and expands these guidelines for all parts of the MOD.

12088. Requisitioning branches or project managers are responsible for the security aspects (including IT security) of any contracts they award and manage. To meet the above policy guidelines, they **must** seek approval (accreditation or confirmation of accreditation) from Info Sy (Industry) 2/3 of any IT system to be used to process protectively marked HMG information (see DMS Vol 3). They will arrange for the approval of any IT systems, the appropriate advice to be given on how the work is to be processed, and on what security and operation procedures will be required to protect the security aspects.

12089. Any ITT or contract must make it clear that approval (accreditation) by an approved HMG authority of any IT system processing protectively marked HMG information is **mandatory.**

This page intentionally left blank.

SECTION II

PROJECT SECURITY PLANNING

Introduction

12090. Integrated Project team (IPT) Leaders are formally responsible for **all** aspects of security for their projects. The purpose of this Section is to outline, for **all** IPT Leaders at **all** levels and their staff in MOD Headquarters, outstations, Commands, Defence Procurement Agency and Agencies, the resources available to assist them in the identification and protection of security aspects of their projects.

12091. Every IPT Leader needs to ensure that the procedure for the award of protectively marked contracts and the protection of work in industry are followed.

12092. Guidance relating to the application of security principles to SMART Procurement can be found on the Acquisition Management System (AMS), available to all project team members

Principles

12093. Reliable security is achieved by:

a. **Correct assessment.** The protective markings applied must be appropriate to the state of development of the project itself, the countermeasures known or anticipated and the progressive disclosure of details as the project materializes.

b. **Need to know.** This rule must be impressed on all concerned both in the Ministry of Defence and in industry.

c. **Co-ordination.** Dispersal of responsibility for project development and deployment brings increased risks and the same standard of security must be applied at all places where a project is being either developed, tested or used.

d. **Review.** The security grading of a project shall be reviewed at each R&D milestone and at least at yearly intervals until the system is brought into service.

These principles will apply to equipment modification as appropriate.

Initial programme phases

120944. Formal indication of Service security requirements will normally be in

the User Requirement, Document (URD) and System Requirement Document (SRD) although some preliminary discussions may have taken place before hand. The security clauses in the URD or SRD are generally stated in broad terms. These need to be amplified when preparing guidance for use in the protection of documents and hardware, preferably in the form of a technical grading guide.

a. It is important for the IPT or project branch associated with a project to prepare a Security Aspects Letter (SAL) and to consult Def Sy (Industry)2/3 and Def Sy (S&T) before approaching any firm prior o the letting of the contract (even for UNCLASSIFIED discussions). This will avoid the embarrassment of negotiations having to be terminated for security reasons.

b. This chapter also describes the security procedures in connection with the award of protectively marked contracts and the protection of work in industry.

c. Assessment phase contracts should require the contractor to examine the broad security requirements set out in the URD or SRD and to report any special precautions and expenditure needed to meet the level of security in the development, testing and production phases for British equipment. Projected foreign sales are likely to require variants with different security criteria.

a. This report must be scrutinized by the IPT (if necessary in consultation with CB Sy 2 and Def Sy (S&T) to check:

(1) That the necessary level of security is possible and achievable in the proposed places of manufacture.

(2) Procedures required for transportation.

(3) Information technology and computer security (see DMS Vol 3).

(4) Electronic emission security (ELSEC Memorandum No 1 issued by CESG).

(5) Other security problems associated with trials.

Preliminaries to the development contract

12095. Preliminaries to the development contract are:

a. Following Assessment Phase the terms of a further SAL should be discussed with Def Sy (S&T) and the contractor, so that it covers any security

matters revealed by the phase. Imposition of special or additional security required after the contract has been let may necessitate revision of the price or the contracts.

b. The definitions set out in a SAL should not leave the firm with any doubts or difficulties concerning its interpretation. The firm's Security Adviser will give detailed guidance to the firm on the way physical, documentary and emission protection requirements are to be met.

c. The SAL for a demonstration phase needs to be in greater detail than that for any earlier phase. The security gradings or requirements must be analyzed and interpreted by the IPT Leader, if necessary in consultation with the Equipment Capability Customer and Def Sy (S&T). The contractor must be advised of the appropriate security gradings to be applied to detailed drawings, assemblies, sub-assemblies and lesser items of hardware and all related documentation. The SAL should be signed by not less than a C1 grade. The advice of Def Sy (S&T) should be sought if any difficulty is encountered in drafting.

d. The IPT Leader should also prepare a detailed protective marking breakdown which, if approved by the appropriate Equipment Grading Committee, will be promulgated in the official grading guide for that equipment.

Review of grading

12096. The Technical Grading Guide is reviewed at least annually by the appropriate grading committee or sub-committee:

a. To identify those aspects of the project which require security grading.

b. Wherever possible, to reduce security gradings as the project progresses; this does not imply that initial standards were set too high but recognizes that not all operational security requirements can be maintained throughout the demonstration and manufacture phases without unacceptable expenditure or disruption to the programme. The IPT Leader must consult Def Sy (S&T) who provide the secretariat of the appropriate grading committee, to initiate these reviews.

Grading committee machinery

12097. The grading committee machinery is:

a. The process of grading equipment for security purposes is controlled by the following committees (see Annex T):

(1) The Naval Equipment Security Committee and its sub-committees, which deal with ships, their propulsion, weapons and ancillary equipment.

(2) The Land Systems Equipment Security Policy Committee and its sub-committees, which deal with most equipment procured for the Army.

(3) The Air Equipment Security Committee and its sub-committees, which deal with aircraft, aircraft engines and ground equipment, avionics and electronics, armaments, together with all guided weapons and nuclear weapons.

(4) The Special Armour Security Committee (SASC).

b. Grading committees are responsible for:

(1) Assigning protective markings to new projects and equipment destined for use by the UK Forces.

(2) Advising on protective markings to new projects and equipment arising from or destined for defence research work.

(3) Keeping existing gradings under review and, when necessary, introducing appropriate amendments.

(4) Advising on the release of defence related data for publication.

c. The Equipment Capability Manager or the Research Director or theIPT Leader, as appropriate, is responsible for notifying the Secretary of the appropriate sub-committee as soon as a project requirement or item of equipment reaches the stage where detailed security gradings need to be promulgated. **Consultation between them is essential.** The Secretary of the committee will obtain from the branches details of items which need to be considered for initial grading or in connection with contractor's publicity.

Project security duties

12098. Project security duties are:

a. For minor projects the security function is normally carried out by the IPT Leader who retains the responsibility of Project Security Officer. For all major projects protected at CONFIDENTIAL or above, a technical officer shall be appointed by the Project Manager to assume the duties of Project Security Officer. He should be familiar with the project, be normally of at least C1 grade, and have a reasonable expectation of continuity in post.

b. The duties of the Project Security Officer include:

(1) The drafting of SALs and the security plan for the project, in consultation as necessary with Info Sy (Industry)2/3, CBSy 2, Info Sy (Tech), Def Sy (S&T) and Equip Sec 3.

(2) Liaison with the Equipment Grading sub-committee and Def Sy (S&T) and where appropriate DESO and PR branches, on matters arising from the interpretation of the Technical Grading Guides and column release schedules (controlled by Def Sy (S&T)).

(3) Representing the Project Manager on the appropriate grading sub-committees and at project progress meetings.

(4) Co-ordination of effective security measures throughout the project.

(5) Occasional spot checks to monitor the application of security measures.

(6) Supervision of the project access list where one exists.

(7) Liaison with Info Sy (Industry)2/3 on the security clearance of contractors and contractor's personnel.

(8) Liaison with CB Sy 2 and R&D establishments' security officers, as appropriate, on the physical security aspects of the project.

Completed and cancelled projects

12099. In contracts subject to DEFCON 659 a contractor is required to protect at the appropriate level any protectively marked information and equipment he holds even after the completion or cancellation of a contract. IPT Leaders must, therefore, inform the contractors concerned of any change in protective marking so that the protection

afforded to the project conforms with the current protective marking of a completed or cancelled project.

Involvement of contractors in security plans

12100. Points concerning the involvement of contractors are as follows:

a. Security should be included on the agenda of progress meetings held with contractors, who should be encouraged to take an active part in determining security gradings. Proposals for regrading which emerge from such discussions should be notified to the appropriate grading committee.

b. Contractors are advised and encouraged to challenge gradings which they believe to be unrealistic or impractical. Such challenges are to be dealt with fully and quickly in consultation with the grading authority.

c. The IPT Leader is responsible for arranging, in the absence of any other action, for the current secret aspects letter to be reviewed once per year.

Open release of official information

12101. Information should only be released to the press through Defence Public Relations staff to whom all requests from the press must be referred. Consultation between the Equipment Capability branch for the project, the IPT Leader, the contractors and the appropriate security grading authority (see para 12100 and Annex T) is essential before any release is made by Defence Public Relations staff. Releases and the conditions on which they are made must be recorded by the Operational Requirements branch and it is essential for this information to be passed to D Def Sy and others involved in the project.

a. Isolated and minor items of information which may not of themselves appear significant may, when placed with information obtained from other sources, result in the publication of a speculative or harmful article of major security importance.

b. Def Sy (S&T) Authored Material is responsible for clearance of matters submitted by Mod staff, contractors and consultants for open publication or for presentation at lectures, seminars, etc or to learned societies, universities, professional bodies, etc at home and abroad.

c. Def Sy (S&T) Pubs & Exhibs is responsible for clearance of UNCLASSIFIED publicity and information brochures, etc produced by the MOD or the defence industry for display at exhibitions or trade shows or for other purposes.

d. The Inventions Unit D Def Sy (S&T) Inv & Pat is responsible for advice to the Patent Office on prohibition for security reasons of the publication of British and foreign patent applications.

e. The procedures governing the release of military information to overseas countries are given in the Manual of Defence Security, chapter 11.

Research programmes

12102. The organization responsible for initiating a research project should seek advice on project security grading from Def Sy (S&T), who will consult the appropriate Service sponsor branch and the Project Manager responsible for the project for which the outcome of the research may eventually be used. Any proposed release of information concerning a research project is to be referred to Def Sy (S&T).

Security of contractor's private venture projects

12103. Notes on private venture projects are at Annex U to this Chapter.

This page intentionally left blank.

ANNEX A TO CHAPTER 12

DEFCON 531 (EDN 10/97)

MINISTRY OF DEFENCE

DISCLOSURE OF INFORMATION

1. 'Information' means any information in any written or other tangible form disclosed to one party by or on behalf of the other party under or in connection with the Contract.

2. Subject to Clause 5 and 6 each party:

a) shall treat in confidence all Information it receives from the other;

b) shall not disclose any of that Information to any third party without the prior written consent of the other party, which consent shall not unreasonably be withheld, except that the Contractor may disclose Information in confidence, without prior consent, to such persons and to such extent as may be necessary for the performance of the Contract;

c) shall not use any of that Information otherwise than for the purpose of the Contract; and

d) shall not copy any of that Information except to the extent necessary for the purpose of exercising its rights of use and disclosure under the Contract.

3. The Contractor shall take all reasonable precautions necessary to ensure that all Information disclosed to the Contractor by or on behalf of the Authority under or in connection with the Contract:

a) is disclosed to its employees and sub-contractors, only to the extent necessary for the performance of the Contract; and

b) is treated in confidence by them and not disclosed except without prior written consent or used otherwise than for the purpose of performing work or having work performed for the Authority under the Contract or any sub-contract under it.

4. The Contractor shall ensure that his employees are aware of his arrangements for discharging the obligations at Clauses 2 and 3 before they receive Information and take such steps as may be reasonably practical to enforce such arrangements.

5. Clauses 2 and 3 shall not apply to any Information to the extent that either party:

a) exercises rights of use or disclosure granted otherwise than in consequence of, or under, the Contract;

b) has the right to use or disclose the Information in accordance with other conditions of the Contract; or

c) can show:

i) that the Information was or has become published or publicly available for use otherwise than in breach of any provision of the Contract or any other agreement between the parties;

ii) that the Information was already known to it (without restrictions on disclosure or use) prior to it receiving it under or in connection with the Contract;

iii) that the Information was received without restriction on further disclosure from a third party who lawfully acquired it and who is himself under no obligation restricting its disclosure; or

iv) from its records that the same information was derived independently of that received under or in connection with the Contract; provided the relationship to any other Information is not revealed.

6. Neither party shall be in breach of this Condition where it can show that any disclosure of Information was made solely and to the extent necessary to comply with a statutory, judicial or parliamentary obligation. Where such a disclosure is made, the party making the disclosure shall ensure that the recipient of the Information is made aware of and asked to respect its confidentiality. Such disclosure shall in no way diminish the obligations of the parties under this Condition.

7. Nothing in this Condition shall affect the parties' obligations of confidentiality where information is disclosed orally in confidence.

ANNEX B TO CHAPTER 12

DEFCON 659 (EDN 9/97)

MINISTRY OF DEFENCE

SECURITY MEASURES

Definition

1. In this Condition:-

a) "**Secret Matter**" means any matter connected with the Contract, or its performance which is designated in writing by the Authority as "Top Secret", "Secret" or "Confidential", and shall include any information concerning the content of such matter and anything which contains or may reveal that matter;

b) "**Employee**" shall include any person who is an employee or director of the Contractor or who occupies the position of a director of the Contractor, by whatever title given.

The Official Secrets Acts

2. The Contractor shall:

a) take all reasonable steps to ensure that all Employees engaged on any work in connection with the Contract have notice that the Official Secrets Acts 1911-1989 apply to them and will continue so to apply after the completion or termination of the Contract; and

b) if directed by the Authority, ensure that any Employee shall sign a statement acknowledging that, both during the term of the Contract and after its completion or termination, he is bound by the Official Secrets Acts 1911-1989 (and where applicable any other legislation).

Security measures

3. Unless he has the written authorisation of the Authority to do otherwise, neither the Contractor nor any of his Employees shall, either before or after the completion or termination of the Contract, do or permit to be done anything which they know or ought reasonably to know may result in Secret Matter being disclosed to or acquired by a person in any of the following categories:

a) who is not a British citizen;

b) who does not hold the appropriate authority for access to the protected matter;

c) in respect of whom the Authority has notified the Contractor in writing that the Secret Matter shall not be disclosed to or acquired by that person;

d) who is not an Employee of the Contractor;

e) who is an Employee of the Contractor and has no need to know the information for the proper performance of the Contract.

4. Unless he has the written authorisation of the Authority to do otherwise, the Contractor and his Employees shall, both before and after the completion or termination of the Contract, take all reasonable steps to ensure that:

a) no photograph of, or pertaining to, any Secret Matter shall be taken and no copy of or extract from any Secret Matter shall be made except to the extent necessary for the proper performance of the Contract;

b) any Secret Matter is at all times strictly safeguarded in accordance with the Manual of Protective Security and upon request, is delivered up to the Authority who shall be entitled to retain it.

A decision of the Authority on the question of whether the Contractor has taken or is taking reasonable steps as required by this Clause, shall be final and conclusive.

5. The Contractor shall:

a) provide to the Authority:

i) upon request, such records giving particulars of those Employees who have had at any time, access to any Secret Matter that is required to be kept in accordance with Sub-clause 4.b.;

ii) upon request, such information as the Authority may from time to time require so as to be satisfied that the Contractor and his Employees are complying with his obligations under this Condition, including the measures taken or proposed by the Contractor so as to comply with his obligations and to prevent any breach of them;

iii) full particulars of any failure by the Contractor and his Employees to comply with any obligations relating to Secret Matter arising under this Condition immediately upon such failure becoming apparent;

b) ensure that, for the purpose of checking the Contractor's compliance with the obligation in Sub-clause 4.b., a representative of the Authority shall be entitled at any time to enter and inspect any premises used by the Contractor which are in any way connected with the Contract and inspect any document or thing in any such premises, which is being used or made for the purposes of the Contract.

Such representative shall be entitled to all such information as he may reasonably require.

6. If at any time either before or after the completion or termination of the Contract, the Contractor or any of his Employees discovers or suspects that an unauthorised person is seeking or has sought to obtain information directly or indirectly concerning any Secret Matter, the Contractor shall forthwith inform the Authority of the matter with full particulars thereof.

Sub-Contracts

7. If the Contractor proposes to make a sub-contract which will involve the disclosure of Secret Matter to the sub-contractor, the Contractor shall:

a) submit for approval of the Authority the name of the proposed subcontractor, a statement of the work to be carried out and any other details known to the Contractor which the Authority shall reasonably require;

b) incorporate into the sub-contract the terms of the Appendix to this condition and such secrecy and security obligations as the Authority shall direct. In the appendix "Agreement" shall mean the "Sub-Contract", "First Party" shall mean the "Contractor" and "Second Party" shall mean the "Sub-Contractor";

c) inform the Authority immediately he becomes aware of any breach by the sub-contractor of any secrecy or security obligation and, if requested to do so by the Authority, terminate the sub-contract.

Termination

8. The Authority shall be entitled to terminate the Contract immediately if:

a) the Contractor is in breach of any obligation under this Condition; or

b) the Contractor is in breach of any secrecy or security obligation imposed by any other contract with the Crown;where the Authority consider the circumstances of the breach jeopardise the secrecy or security of the Secret Matter.

This page intentionally left blank.

APPENDIX TO DEFCON 659 (EDN 9/97)

MINISTRY OF DEFENCE

SECURITY MEASURES

PROVISIONS TO BE INCLUDED IN RELEVANT SUB-CONTRACTS

Definition

1. In this Condition:-

a. "**Secret Matter**" means any matter connected with the Agreement, or its performance which the First Party informs the Second Party in writing has been designated by the Authority as "Top Secret", "Secret" or "Confidential", and shall include any information concerning the content of such matter and anything which contains or may reveal that matter;

b. "**Employee**" shall include any person who is an employee or director of the Second Party or who occupies the position of a director of the Second Party, by whatever title given.

c. The "**Authority**" means the Secretary of State for Defence.

The Official Secrets Acts

2. The Second Party shall:

a. Take all reasonable steps to ensure that all Employees engaged on any work in connection with the Agreement have notice that the Official Secrets Acts 1911-1989 apply to them and will continue so to apply after the completion or termination of the Agreement; and

b. If directed by the First Party or the Authority, ensure that any Employee shall sign a statement acknowledging that, both during the term of the Agreement and after its completion or termination, he is bound by the Official Secrets Acts 1911-1989 (and where applicable any other legislation).

Security Measures

3. Unless he has the written authorisation of the Authority to do otherwise, neither the Second Party nor any of his Employees shall, either before or after the completion or termination of the Agreement, do or permit to be done anything which they know or ought reasonably to know may result in Secret Matter being disclosed to or acquired by a person in any of the following categories:

a. who is not a British citizen;

b. who does not hold the appropriate authority for access to the protected matter;

c. in respect of whom the Authority has notified the Second Party in writing that the Secret Matter shall not be disclosed to or acquired by that person;

d. who is not an Employee of the Second Party;

e. who is an Employee of the Second Party and has no need to know the information for the proper performance of the Agreement.

4. Unless he has the written permission of the Authority to do otherwise, the Second Party and his Employees shall, both before and after the completion or termination of the Agreement, take all reasonable steps to ensure that:

a. no photograph of, or pertaining to, any Secret Matter shall be taken and no copy of or extract from any Secret Matter shall be made except to the extent necessary for the proper performance of the Agreement;

b. any Secret Matter is at all times strictly safeguarded in accordance with the Manual of Protective Security and upon request, is delivered up to the Authority who shall be entitled to retain it.

A decision of the Authority on the question of whether the Second Party has taken or is taking reasonable steps as required by this Clause, shall be final and conclusive.

5. The Second Party shall:

a. provide to the Authority:

i) upon request, such records giving particulars of those Employees who have had at any time, access to any Secret Matter that is required to be kept in accordance with Sub-clause 4.b.;

ii) upon request, such information as the Authority may from time to time require so as to be satisfied that the Second Party and his Employees are complying with his obligations under this Condition, including the measures

taken or proposed by the Second Party so as to comply with his obligations and to prevent any breach of them;

iii) full particulars of any failure by the Second Party and his Employees to comply with any obligations relating to Secret Matter arising under this Condition immediately upon such failure becoming apparent;

b. ensure that, for the purpose of checking the Second Party's compliance with the obligation in Sub-clause 4.b., a representative of the First Party or the Authority shall be entitled at any time to enter and inspect any premises used by the Second Party which are in any way connected with the Agreement and inspect any document or thing in any such premises, which is being used or made for the purposes of the Agreement. Such representative shall be entitled to all such information as he may reasonably require.

6. If at any time either before or after the completion or termination of the Contract, the Second Party or any of his Employees discovers or suspects that an unauthorised person is seeking or has sought to obtain information directly or indirectly concerning any Secret Matter, the Second Party shall forthwith inform the Authority of the matter with full particulars thereof.

Sub-Contracts

7. If the Second Party proposes to make a sub-contract which will involve the disclosure of Secret Matter to the sub-contractor, the Second Party shall:

a. submit for approval of the Authority the name of the proposed sub-contractor, a statement of the work to be carried out and any other details known to the Second Party which the Authority shall reasonably require;

b. incorporate into the sub-contract the terms of this Condition and such secrecy and security obligations as the Authority shall direct.

c. inform the Authority immediately he becomes aware of any breach by the sub-contractor of any secrecy or security obligation and, if requested to do so by the Authority, terminate the Agreement.

Termination

8. The First Party shall be entitled to terminate the Agreement immediately if:

a. the Second Party is in breach of any obligation under this Condition; or

b. the Second Party is in breach of any secrecy or security obligation imposed by any other contract with the Crown;

where the Authority consider the circumstances of the breach jeopardise the secrecy or security of the Secret Matter and notifies its contractor accordingly.

ANNEX C

DEFCON 76 (EDN 10/97)

MINISTRY OF DEFENCE

CONTRACTOR'S PERSONNEL AT GOVERNMENT ESTABLISHMENTS

Definitions

1. Reference herein to:

a) "Government Establishment" or "site" shall be deemed to include any of Her Majesty's Ships or Vessels and Service Stations; and

b) "Officer in Charge" shall be deemed to include Officers Commanding Service Stations, Ships' Masters or Senior Officers, and Heads of Government Establishments.

General

2.

a) The Officer in Charge shall provide such available administrative and technical facilities for the Contractor's representatives employed at Government Establishments for the purpose of the Contract as may be necessary for the effective and economical discharge of work under the Contract. These facilities will be provided free of charge unless otherwise stated in the Contract. The status to be accorded to the Contractor's representatives for messing purposes will be at the discretion of the Officer in Charge.

b) Any land or premises (including temporary buildings) made available to the Contractor by the Authority in connection with the Contract shall be made available to the Contractor free of charge, unless otherwise stated in the Contract, and shall be used by the Contractor solely for the purpose of performing the Contract. The Contractor shall have the use of such land or premises as licensee and shall vacate the same upon completion of the Contract. Any utilities required by the Contractor shall be subject to the charges set out in the Contract.

c) The Contractor shall have no claim against the Authority for any additional cost or delay occasioned by the closure for holidays of Government Establishments, where this is made known to him prior to placing the Contract.

Liability in respect of damage to Government property

3. Without prejudice to the provisions of Standard Condition 11 (Issues of Government Property) and Standard Condition 12 (Loss of or Damage to the Articles) of Form GC/STORES/1, where those Conditions form part of the Contract, the Contractor shall, except as otherwise provided for in the Contract, make good or, at the option of the Authority, pay compensation for all damage occurring to any Government Property, which includes land or buildings, occasioned by the Contractor, or by his servants, agents or sub-contractors, arising from his or their presence on a Government Establishment in connection with the Contract, provided that this Condition shall not apply to the extent that the Contractor is able to show that any such damage was not caused or contributed to by any circumstances within his reasonable control or of that of his servants, agents or sub-contractors.

4. The total liability of the Contractor under Condition 3 herein shall be subject to any limitation specified in the Contract.

Contractor's property

5. All property of the Contractor while at a Government Establishment shall be at the risk of the Contractor, and the Authority shall accept no liability for any loss or damage howsoever occurring thereto or caused thereby, except as follows:-

a) where any such loss or damage was caused or contributed to by any act, neglect or default of any Government Servant, agent or contractor then the Authority shall accept liability therefore to the extent to which such loss or damage is so caused or contributed to as aforesaid; and

b) where any property of the Contractor has been taken on charge by the Officer in Charge, and a proper receipt has been given therefore, then the Authority shall be liable for any loss or damage occurring to that property while held on such charge as aforesaid.

Contractor's representatives

6. The Contractor shall submit in writing to the Authority for approval, initially and as necessary from time to time, a list of the representatives who may need to enter a Government Establishment for the purpose of, or in connection with, work under the

Contract, giving such particulars as the Authority may require, including full details of birthplace and parentage of any representative who:

a) was not born in the United Kingdom; or

b) if he was born in the United Kingdom, was born of parents either or both of whom were not born in the United Kingdom.

7. The Authority will issue passes for those representatives who are approved by him in accordance with Condition 6 herein for admission to a Government Establishment and a representative shall not be admitted unless in possession of such a pass. Passes shall remain the property of the Authority and shall be surrendered on demand or on completion of the work

8. Notwithstanding the provisions of Conditions 6 and 7 hereof if, in the opinion of the Authority, any representative or agent of the Contractor shall misconduct himself, or it shall not be in the public interest for any person to be employed or engaged by the Contractor, the Contractor shall remove such person without delay on being required to do so and shall cause the work to be performed by such other person as may be necessary.

9. The decision of the Authority upon any matter arising under Conditions 6 to 8 shall be final and conclusive.

Observance of regulations

10.

a) The Contractor shall be responsible for ensuring that his representatives have the necessary probity (by undertaking a Basic Check) and, where applicable, are cleared to the appropriate level of security when employed within the boundaries of a Government Establishment. The Contractor's representatives shall comply with such rules, regulations and requirements as may be in force whilst at that Establishment.

b) Where the Contractor requires information on the Basic Check procedure or security clearance for his representative and/or is not in possession of the relevant rules, regulations and requirements and/or requires guidance thereon, he shall apply in the first instance to the Project Manager/Equipment Support Manager.

c) When on board ship, compliance with the rules, regulations and requirements shall be in accordance with the Ship's Regulations as interpreted by the Officer in Charge. Details of such rules, regulations and requirements shall be provided on request by the Officer in Charge.

Transport overseas

11. Where the Contractor's representatives are required by the Contract to join or visit a Government Establishment overseas, transport between the United Kingdom and the place of duty (but excluding transport within the United Kingdom) shall be provided free of charge by the Authority whenever possible, normally by Royal Air Force or by MOD chartered aircraft. The Contractor shall make such arrangements through the Project Manager/Equipment Support Manager named for this purpose in the Contract. When such transport is not available within a reasonable time, or in circumstances where the Contractor wishes his representatives to accompany materiel for installation which he is to arrange to be delivered, the Contractor shall make his own transport arrangements. The Authority shall reimburse the Contractor's costs for such transport of his representatives on presentation of evidence supporting the use of alternative transport and of the cost involved. Transport of the Contractor's representatives locally overseas which is necessary for the purposes of the Contract shall be provided wherever possible by the Authority and, where so provided, will be free of charge.

Medical treatment overseas

12. Out-patient medical treatment given to the Contractor's representatives by a Service Medical Officer or other Government Medical Officer at a Government Establishment overseas shall be free of charge. Treatment in a Service hospital or medical centre, dental treatment, the provision of dentures or spectacles, conveyance to and from a hospital, medical centre or surgery not within the Establishment, and transportation of the Contractor's representatives back to the United Kingdom, or elsewhere, for medical reasons, shall be charged to the Contractor at rates fixed in accordance with current MOD regulations.

Injuries, disease and dangerous occurrences

13. Any injury, disease or dangerous occurrence involving Contractor's employees, representatives, agents or equipment which requires to be reported under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1985 shall be reported by the Contractor to the Officer in Charge in addition to any report which it is the responsibility of the Contractor to make to the Health and Safety Executive.

Dependants of contractor's representatives

14. No assistance from public funds, and no messing facilities, accommodation or transport overseas shall be provided for dependants or members of the families of the

Contractor's representatives. Medical or necessary dental treatment may, however, be provided for dependants or members of families on repayment at current MOD rates.

Provision of funds overseas

15. The Contractor shall, wherever possible, arrange for funds to be provided to his representatives overseas through normal banking channels (eg by travellers cheques). If banking or other suitable facilities are not available, the Authority shall, upon request by the Contractor and subject to any limitation required by the Contractor, make arrangements for payments, converted at the prevailing rate of exchange (where applicable), to be made by the Establishment to which the Contractor's representatives are attached. All such advances made by the Authority shall be recovered from the Contractor.

Special Health and Safety hazards

16.

a) The Contractor shall notify the nominated site project liaison officer or overseeing officer of any special health or safety hazards which might be involved in the work to be performed and shall advise him of any precautions that ought to be taken.

b) The Authority shall notify the Contractor of any special health or safety hazards which might be encountered on the Government Establishment by the Contractor and shall advise him of any precautions that ought to be taken.

c) The Contractor shall draw to the attention of his employees, sub-contractors, the employees of sub-contractors and all other persons under his control:

i) All hazards required to be notified under sub-clause a. above; and

ii) All hazards of which the Authority gives him notice.

d) The Contractor shall take all steps necessary to ensure that such persons are adequately instructed on such hazards and any associated safety measures.

e) The Contractor shall provide to the nominated site project liaison officer or overseeing officer:

i) Copies of the section of his own and sub-contractors safety policies relevant to hazards notified under sub-clause a. above; and

ii) Copies of notifications and instructions issued under sub-clauses b. and c. above.

This page intentionally left blank.

ANNEX D TO CHAPTER 12

MEMORANDUM

TO: Info Sy (Industry)2/3 ROOM 312 St Giles Court 1-13 St Giles High Street London WC2H 8LD	FROM: REF NO: DATE

REQUEST FOR CONFIRMATION OF SECURITY STATUS OF A UK CONTRACTOR

LEVEL OF PROTECTED INFORMATION TO BE RELEASED TO THE CONTRACTORS (TICK APPROPRIATE BOXES)

TOP SECRET	SECRET	CONFIDENTIAL	ATOMIC	UK EYES ONLY	UK EYES DISCRETION	OTHERS (STATE WHICH)

SERIAL NO	COLUMN A (TO BE COMPLETED BY REQUISITIONING BRANCH)	COLUMN B (TO BE COMPLETED BY INFO SY (INDUSTRY))	COLUMN C (TO BE COMPLETED BY INFO SY (INDUSTRY))
	NAME AND ADDRESS OF CONTRACTORS PREMISES	NAME OF SECURITY OFFICER AND ADDRESS IF DIFFERENT FROM COLUMN A	LIST X STATUS AND LEVEL OF CLEARANCE

(CONTINUE ON A SEPARATE SHEET IF NECESSARY)

NB. When column 'C' indicates that a contractor holds only a provisional clearance a separate letter will be attached. Where no clearance exists see Sub-section IC.

FOR INFO SY (INDUSTRY) USE SIGNED: DATE:
STAMP:

This page intentionally left blank.

ANNEX E TO CHAPTER 12

LETTER TO CONTRACTOR REQUESTING COMPLETION OF FORMS SECURITY QUESTIONNAIRE

Personal to:

1. Please refer to our recent discussions/correspondence concerning the possibility of your company undertaking work for the Ministry of Defence.

2. As it may be necessary for members of your company to be granted access to protected information in the course of the tender or contract, it will be necessary for yourself and perhaps one or two other members to be authorised for such access in advance.

3. I should, therefore, be grateful if you would complete, in duplicate the enclosed Security Questionnaire in respect of yourself. If necessary you should also arrange for the completion of Security Questionnaires in respect of one or two members of staff whose services will required in the preparation of the tenders. This personal information should be obtained from company records wherever possible.

This page intentionally left blank.

ANNEX F TO CHAPTER 12

LETTER TO CONTRACTOR REQUESTING COMPLETION OF OSA FORMS

Personal to:

1. Please refer to my letter of.....
reference ..... concerning the approval of certain members of your company for access to protected information.

2. You should be aware that any protected information which may be disclosed under this tender/contract is entrusted to you in strict confidence. It is protected by and its recipients will be subject to the Official Secrets Acts 1911 to 1989. This applies whether or not a contract or subcontract is eventually placed with you.

3. Can I please therefore ask you [and the other 2 employees Mr ..... and Mr .....] to complete the enclosed Official Secrets Acts Form E74 in duplicate, retaining one copy and returning the other to me at the above address.

Yours sincerely

This page intentionally left blank.

ANNEX G TO CHAPTER 12

SECURITY ASPECTS LETTER FOR INVITATIONS TO TENDER TO UK CONTRACTORS CURRENTLY ON LIST X

(PROTECTIVE MARKING)

Messrs .....

For the personal attention of:
(Name of company Security Controller)

Dear Sir

TENDER NO_____(to be inserted by the Contracts staff)

1. On behalf of the Secretary of State for Defence, I hereby give you notice that any sketch, model, article, note or document, or information connected with or arising out of the above-mentioned Invitation to Tender, is subject to the provisions of the Official Secrets Acts 1911-1989. Your attention is particularly drawn to the following specific aspects which must be fully safeguarded:

	PROTECTIVE MARKING		ASPECTS
a.	To be disclosed to firms submitting tenders	)Note:	Either of these headings may be used or adapted as appropriate.
b.	To be disclosed to the successful bidder only	)	

2. Will you please confirm that:

a. This definition of the protected aspects of the above Invitation to Tender has been brought to the attention of the person directly responsible for the security of this tender.

b. The definition is fully understood.

c. Measures can, and will, be taken to safeguard the protected aspects.

(PROTECTIVE MARKING)

(PROTECTIVE MARKING)

3. If you have any difficulty either in interpreting this definition of the protected aspects or in safeguarding them, will you please let me know immediately, and send a copy of your letter to your Security Adviser.

4. In the event of a contract being placed with you, these aspects would constitute `SECRET matter' for the purpose of clause1 a) of Def Con 659 - Security Measures.

5. Any access to protected information on MOD premises that may be needed will be subject to MOD security regulations under the discretion of the MOD Project Officer.

Yours faithfully

Copy to: Info Sy (Industry)2/3
Def Sy (S&T)

(PROTECTIVE MARKING)

ANNEX H TO CHAPTER 12

SECURITY ASPECTS LETTER FOR INVITATIONS TO TENDER TO UK CONTRACTORS WHERE PROVISIONAL MOD SECURITY APPROVAL FOR THE COMPANY HAS BEEN GRANTED AND WHERE CONFIDENTIAL OR ABOVE NEEDS TO BE DISCLOSED AT THE TENDER STAGE

(PROTECTIVE MARKING)

Messrs .....

For the personal attention of:
(Name of company's approved recipient)

Dear Sirs

TENDER NO _____ (to be inserted by Contracts staff)

1. On behalf of the Secretary of State for Defence, I hereby give you notice that any sketch, plan, model, article, note or document, or information connected with or arising out of the above-mentioned Invitation to Tender, is subject to the provisions of the Official Secrets Acts 1911-1989. Your attention is particularly drawn to the following specific aspects which must be fully safeguarded:

PROTECTIVE MARKING		ASPECTS
a. To be disclosed to firms submitting tenders	)	Either of these headings may be used or adapted as appropriate.
b. To be disclosed to the successful bidder only (describe in non-specific terms if possible)	)	

Note:

2. A copy of a Memorandum on Security for Contractors, which outlines the principal measures required to safeguard protected information, is enclosed. Your particular attention is drawn to paragraph 12 of the Memorandum, and I should be grateful if you would send to the Technical Authority, on MOD SECURITY

(PROTECTIVE MARKING)

(PROTECTIVE MARKING)

QUESTIONNAIRE(s) Forms (available on request), personal details of any other members of your firm to whom you need to disclose information marked CONFIDENTIAL or above in order to complete your tender. The number of such other persons should be restricted to the fewest possible, and they should not in any case be allowed access to information marked CONFIDENTIAL or above until they have been approved by the Ministry.

3. Will you please confirm that:

a. The above is fully understood.

b. Measures can, and will, be taken to safeguard the protected aspects.

4. If you have any difficulty either in interpreting this definition of the protected aspects or in safeguarding them, will you please let me know immediately.

5. In the event of a contract being placed with you, the above aspects would constitute `secret matter' for the purpose of clause 1 a) of Def Con 659 - Security Measures.

6. Any access to protected information on MOD premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Officer.

Yours faithfully

Copy to: Info Sy (Industry)2/3
Def Sy (S&T)

(PROTECTIVE MARKING)

ANNEX I TO CHAPTER 12

SECURITY ASPECTS LETTER FOR INVITATIONS TO TENDER TO UK CONTRACTORS WHERE PROVISIONAL MOD APPROVAL HAS BEEN GRANTED FOR THE CONTRACTOR BUT NO INFORMATION ABOVE RESTRICTED NEEDS TO BE DISCLOSED AT THE TENDER STAGE

PROTECTIVE MARKING
(not higher than RESTRICTED)

Messrs .....

For the attention of:
(Name of company's approved recipient)

Dear Sir

TENDER NO _____ (to be inserted by the Contracts staff)

1. On behalf of the Secretary of State for Defence, I hereby give you notice that any sketch, plan, model, article, note or document, or information connected with or arising out of the above-mentioned Invitation to Tender, is subject to the provisions of the Official Secrets Acts 1911-1989.

2. In the event of a contract being placed with you, the following aspects would constitute `secret matter' for the purpose of clause 1 a) of Def Con 659 - Security Measures..

PROTECTIVE MARKING	ASPECTS
a. RESTRICTED (to be disclosed to tendering firms)	
b. (To be disclosed to the contractor)	**Note:** Describe Aspects at CONFIDENTIAL and above in non-specific terms.

PROTECTIVE MARKING
(not higher than RESTRICTED)

PROTECTIVE MARKING
(not higher than RESTRICTED)

3. The enclosed form, which outlines the principal measures required to safeguard RESTRICTED information, is attached for your information.

4. Will you please confirm that measures can and will be taken as necessary to safeguard the protective aspects referred to above.

Yours faithfully

Copies to: Info Sy (Industry)2/3
Def Sy (S&T)

ANNEX J TO CHAPTER 12

SECURITY ASPECTS LETTER FOR CONTRACTS AT CONFIDENTIAL AND ABOVE TO LIST X CONTRACTORS

(PROTECTIVE MARKING)

Messrs .....

For the personal attention of:
(Name of company Security Officer)

Dear Sirs

CONTACT NO _____ DATE OF CONTRACT
(to be inserted by the Contracts staff)

1. On behalf of the Secretary of State for Defence. I hereby give you notice that the following aspects are designated `Secret Matter' for the purpose of clause1 a) of Def Con 659 - Security Measures included in the above contract:

PROTECTIVE MARKING ASPECTS

2. Will you please confirm that:

a. The above definition of the Secret Matter of the above contract has been brought to the attention of the person directly responsible for the security of this contract.

b. The definition is understood.

c. Measures can, and will be taken to safeguard the Secret Matter.

3. If you have any difficulty either in interpreting the definition of the Secret Matter or in safeguarding it, will you please let me know immediately, and send a copy of your letter to your Security Adviser.

4. Any access to information on MOD premises that may be needed, will be in accordance with MOD security regulations under the direction of the MOD Project Officer.

Yours faithfully

Copies to:
Info Sy (Industry)2/3
Def Sy (S&T)

(PROTECTIVE MARKING)

This page intentionally left blank.

ANNEX K TO CHAPTER 12

SECURITY ASPECTS LETTER FOR CONTRACTS TO UK FIRMS WITH PROVISIONAL MOD SECURITY CLEARANCE

(PROTECTIVE MARKING)

Messrs .....

For the personal attention of:
(Name of company's approved recipient)

Dear Sirs

CONTRACT NO _____ DATE OF CONTRACT
(to be inserted by the Contracts staff)

1. On behalf of the Secretary of State for Defence, I hereby give you notice that the following aspects are designated `Secret Matter' for the purpose of clause 1 a) of Def Con 659 - Security Measures included in the above contract:

PROTECTIVE MARKING ASPECTS

2. A copy of a Memorandum on Security for Contractors, which outlines the principal measures required to safeguard protected information, is enclosed. Your particular attention is drawn to paragraph 12 of the Memorandum, and I should be grateful if you would send to the Technical Authority, on MOD SECURITY QUESTIONNAIRE Forms (available on request), personal details of any other members of your firm to whom you need to disclose information marked CONFIDENTIAL or above. The number of such other persons should be restricted to the fewest possible, and they should not in any case be allowed access to information marked CONFIDENTIAL or above until they have been approved by the Ministry.

3. Will you please confirm that:

a. The above definition of the Secret Matter of the contract is understood.

b. Measures can, and will, be taken to safeguard the Secret Matter.

If you have any difficulty either in interpreting the definition of the Secret Matter or in safeguarding it, or in any other respect, will you please let me know immediately.

(PROTECTIVE MARKING)

4. Any access to information on MOD premises that may be needed will be in accordance with MOD security regulations under the direction of the MOD Project Officer.

Yours faithfully

Copies to:
Info Sy)industry)2/3
Def Sy (S&T)

ANNEX L TO CHAPTER 12

SECURITY ASPECTS LETTER - CHANGE TO OR AMENDMENT OF A SECURITY ASPECTS LETTER

(PROTECTIVE MARKING)

Messrs .....

For the personal attention of:
(Name of company's Security Officer)

Dear Sirs

CONTRACT NO _____ DATE OF CONTRACT
(to be inserted by Requisitioning Branch)

Reference: Letter reference ..... dated ..... (the letter to be cancelled)

1. On behalf of the Secretary of State for Defence, I hereby give you notice that the following aspects are designated `Secret Matter' for the purpose of clause 1 a) of Def Con 659 - Security Measures included in the above contract:

PROTECTIVE MARKING ASPECTS

2. Will you please confirm that:

a. This re-definition of the Secret Matter of the above contract has been brought to the attention of the person directly responsible for the security of this contract.

b. Measures can, and will, be taken to safeguard the Secret Matter.

3. If you have any difficulty either in interpreting the definition of the Secret Matter or in safeguarding it, will you please let me know immediately, and send a copy of your letter to your Security Adviser.

4. Access to information on MOD premises that may be need will be in accordance with MOD security regulations under the direction of the MOD Project Officer.

Yours faithfully

Copies to:
Info Sy (Industry)2/3
Def Sy (S&T)

(PROTECTIVE MARKING)

This page intentionally left blank.

ANNEX M TO CHAPTER 12

DOUBTFUL GRADINGS

From:	....	To	....
	....		....
	....		....
	....		....

Subject Reference Number ....

Dear Sir

We acknowledge receipt of your letter/report on the above subject which is receiving attention. The reason for the grading of .... is not, however, clear to us.

From our knowledge of the subject and the written definition of the secret matter in the Security Aspects Letter, reference .... we should have considered a grading of .... more appropriate.

If you agree with this would you please let us know so that we may re-grade the document.

If, on the other hand, you confirm that your grading is correct we should be much obliged if you would, in due course, amend the Security Aspects Letter so that we know precisely what information must be safeguarded under Def Con 659.

Our Security Adviser has asked us to use this form when in doubt about a grading and to send him a copy.

Yours faithfully

Copy to:

Info Sy (Industry)2/3
Def Sy (S&T)

This page intentionally left blank.

ANNEX N TO CHAPTER 12

(PROTECTIVE MARKING)

MEMORANDUM

TO: INFO SY (INDUSTRY)1 ROOM 312 ST GILES COURT 1-13 ST GILES HGH STREET LONDON WC2H 8D	FROM: Insert full name and address of requisitioning branch or contracts branch as appropriate.

REQUEST FOR SECURITY APPROVAL TO PLACE A PROTECTIVELY MARKED CONTRACT OVERSEAS

A. Full Name and Address of Contractor	B. Full Name and Address of Place of Manufacture (if Different from A.)

C. Maximum Level of Release of Protectively Marked Material:

D. Name of Project:

E. Is the Contract Associated with an International Collaborative Project? YES/NO

Is the Project Governed by a MOU? YES/NO

I Confirm that all Protectively Marked Material Relating to the Proposed Contract/Tender will be Approved for Release Overseas in Accordance with JSP 440, Chapter 12, Sub-Section I.

Signed:

Date:

This page intentionally left blank.

ANNEX O TO CHAPTER 12

SECURITY ASPECTS LETTER FOR INVITATIONS TO TENDER TO OVERSEAS FIRMS APPROVED BY INFO SY (INDUSTRY)1 FOR RELEASE OF INFORMATION AT THE APPROPRIATE PROTECTIVE MARKING

(PROTECTIVE MARKING)

Messrs .....

For the personal attention of:
(Company Security Controller)

Dear Sir

TENDER NO _____(to be inserted by the Contracts staff)

1. Referring to the above quoted Invitation to Tender, and in particular paragraph ..... I hereby give you notice that the classified aspects, which are entrusted to you in confidence are as follows:-

CLASSIFICATION (Note: The Prefix UK ..... will be needed)		ASPECTS
a. To be disclosed to firms submitting tenders	)	Either of these headings may be used or adapted as appropriate. The description of Aspects at b to be in non-specific terms if possible.
b. To be disclosed to the successful bidder only	)	

Note

2. Any access to classified information on Ministry of Defence (MOD) premises that may be needed will be subject to MOD security regulations under the direction of the MOD Project Officer.

3. You are requested to acknowledge receipt of this letter confirming that:

a. The definition of the classified matter is understood and has been brought to the attention of the person directly responsible for the security of the tender.

(PROTECTIVE MARKING)

b. Measures can, and will, be taken to safeguard the classified matter as set out above and in the tender documents.

4. Any difficulties experienced in interpreting and implementing the above should be reported immediately to me.

Yours faithfully

Copies to:
Info Sy (Industry)1
Def Sy (S&T)

ANNEX P TO CHAPTER 12

SECURITY ASPECTS LETTER FOR CONTRACTS TO OVERSEAS FIRMS APPROVED BY INFO SY (INDUSTRY)1 FOR RELEASE OF INFORMATION AT THE APPROPRIATE PROTECTIVE MARKING

(PROTECTIVE MARKING)

Messrs

For the personal attention (Company Security Controller)

CONTRACT NO _____ (to be completed by Contract staff)

1. With reference to paragraph ____ of the attached contracts document, I hereby give you notice that the classified matter is as follows:

CLASSIFICATION ASPECTS

(Note: The prefix UK _____ will be needed)

2. Any access to information on Ministry of Defence premises that may be needed will be in accordance with MOD security regulations under the direction of the Ministry of Defence Project Officer.

3. You are requested to acknowledge receipt of this letter confirming that:

a. The definition of the classified matter is understood and has been brought to the attention of the person directly responsible for the security of the contract.

b. The requirement and obligations set out above and in the contract document can and will be met.

4. Any difficulties experienced or expected in interpreting and implementing the above should be reported immediately to me.

Yours faithfully

Copies to:
Info Sy (Industry)1
Def Sy (S&T)

(PROTECTIVE MARKING)

This page intentionally left blank.

ANNEX Q TO CHAPTER 12

RESTRICTED SECURITY CONDITIONS OVERSEAS

Definitions

1. The term "Authority" means Contracting Authority.

Security grading

2. The Authority shall issue a RESTRICTED Aspects Letter which shall define the RESTRICTED matter that is furnished, or which is to be developed, under this Contract. The Contractor shall mark all RESTRICTED documents which he originates or copies during the Contract with the equivalent national grading.

Protection of RESTRICTED information

3. Except with the consent in writing of the Authority, the Contractor shall not disclose the Contract or any provision thereof to any person other than a person employed by the Contractor. It must be confined to those members of the staff whose access to the information is essential for the purpose of his duties.

4. Except with the consent in writing of the Authority the Contractor shall not make use of the Contract or any information issued or furnished by or on behalf of the Authority otherwise than for the purpose of the Contract, and, save as provided for in Clause 5 the Contractor shall not make any article or part thereof similar to the Articles for any other purpose.

5. Subject to any rights of Third Parties, nothing in this Condition shall, however, constrain the use for any purpose by the Contractor of any specifications, plans, drawings and other documents, the rights of which vest in him otherwise than as a result of work carried out under this Contract.

6. Any samples or patterns or any specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and must be returned on completion of the Contract.

7. When not in use RESTRICTED documents should be stored under lock and key.

Loss

8. Any loss of a RESTRICTED document should be reported without delay to the Authority.

Transmission

9. RESTRICTED documents should be transmitted in such a way as to ensure that no unauthorised person has access. Commercial Couriers may be used, however, transmission via public networks such as the Internet or any other form of electronic connectivity is not permitted without the use of encryption mutually acceptable to the appropriate security authorities.

ANNEX R TO CHAPTER 12

RESTRICTED SECURITY CONDITIONS UK

Definitions

1. The term "Authority" means Contracting Authority.

Security grading

2. The Authority shall issue a RESTRICTED Aspects Letter which shall define the RESTRICTED matter that is furnished, or which is to be developed, under this Contract. The Contractor shall mark all RESTRICTED documents which he originates or copies during the Contract with the equivalent national grading.

Official Secrets Acts

3. The Contractor's attention is drawn to the provisions of the Official Secrets Acts 1911 to 1989 in general, and to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1989) in particular. The Contractor shall take all reasonable steps to ensure that all persons employed on any work in connection with the Contract have notice that these statutory provisions apply to them and will continue so to apply after the completion or earlier termination of the Contract.

Protection of RESTRICTED information

4. Disclosure of RESTRICTED information must be strictly in accordance with the "need to know" principle. Except with the written consent of the Authority, the Contractor shall not disclose the Contract or any provision thereof to any person other than a person employed by the Contractor. It must be confined to those members of the staff whose access to the information is essential for the purpose of his duties.

5. When not in use RESTRICTED documents should be stored under lock and key.

Transmission of RESTRICTED information

6. RESTRICTED documents should be transmitted, both within and outside company premises in such a way as to ensure that no unauthorised person has access. They may be sent by ordinary post in a single envelope. The word RESTRICTED should **NOT** appear on the envelope. The envelope should bear a company stamp that clearly indicates the full address of the office from which it was sent.

7. Advice on the transmission of RESTRICTED documents abroad or any other general advice including the transmission of RESTRICTED hardware should be sought from the Authority.

Loss

8. Any loss of RESTRICTED information should be reported without delay to the Authority.

ANNEX S TO CHAPTER 12

SECURITY ASPECTS LETTER FOR A CONTRACT INVOLVING INFORMATION PROTECTIVELY MARKED RESTRICTED BUT NOT ABOVE, TO UK FIRMS

(PROTECTIVE MARKING)

Messrs .....

For the personal attention of:
(Name of company Security Controller if List X;
Name of responsible Officer if not List X)

Dear Sirs

CONTRACT NO _____ DATE OF CONTRACT
(to be inserted by Contracts Branch)

1. On behalf of the Secretary of State for Defence I hereby give you notice that the following aspects of the work under the above contract are marked **RESTRICTED:**

2. Will you please confirm that the definition is understood.

3. I have to remind you that information about this contract must not without the approval of the Authority be published or communicated to anyone except where necessary for the execution of the contract.

4. Your attention is drawn to the provisions of the Official Secrets Acts 1911-1989 in general, to the provisions of Section 2 of the Official Secrets Act 1911 (as amended by the Act of 1920) in particular, that you should take all reasonable steps to ensure that all persons employed on any work in connection with the contract have notice that these statutory provisions apply to them and will continue so to apply after the completion or earlier determination of the contract.

5. Any access to information on MOD premises that may be needed will be in accordance with MOD security regulations under the direction of the MOD Project Officer.

(PROTECTIVE MARKING)

(PROTECTIVE MARKING)

6. The enclosed form, which outlines the principal measures required to safeguard RESTRICTED information is attached for your information.

Yours faithfully

ANNEX T TO CHAPTER 12

COMMITTEES APPOINTED FOR THE SECURITY GRADING OF DEFENCE EQUIPMENT AND TECHNOLOGY.

1. **Naval Equipment Security Committee:**

Chairman	:	Equipment Capability Manager
Secretary	:	ESB (Sea) Equip Sec 3

Naval Equipment Security Sub-Committees

NEGC 2	:	Communications, Command and Control, and Electronic Warfare
Chairman	:	Equipment Capability Manager
NEGC 3	:	Above Water Warfare
Chairman	:	Equipment Capability Manager
NEGC 4	:	Under Water Warfare
Chairman	:	Equipment Capability Manager
NEGC 5	:	Ship construction, engineering and NBCD
Chairman	:	Equipment Capability Manager
NEGC 6	:	Naval Aviation
Chairman	:	Equipment Capability Manager

2. Land Systems Equipment Security Policy Committee

Chairman	:	Equipment Capability Manager
Secretary	:	ESB (Land) Equip Sec 3

Army Equipment Grading Sub-Committees: Eight grading sub-committees have been appointed with responsibilities as shown:

a. Fighting Vehicle Grading Sub-Committee (FVGS) - with responsibility for armoured fighting vehicles and APCs, their associated weapon systems and "B" vehicles.

Chairman : Equipment Capability Manager

b. Close Combat Weapons Grading Sub-Committee (CCWGS) - with responsibility for close combat and anti-armour weapons and infantry equipment.

Chairman : Equipment Capability Manager

c. Engineer Equipment Grading Sub-Committee (EEGS) - with responsibility for general engineer equipment, mines and demolition equipment.

Chairman : Equipment Capability Manager

d. NBC Grading Sub-Committee (NBCGS) - with responsibility for NBC defence equipment.

Chairman : Equipment Capability Manager

e. Artillery Weapons Grading Sub-Committee (Arty WGS) - with responsibility for artillery fire support and air defence, artillery fire control equipment and artillery ADP systems.

Chairman : Equipment Capability Manager

f. Army Communications Grading Sub-Committee (A Comms GS) - with responsibility for Army signals equipment, communications security equipment in use by the army (prime responsibility in this field rests with CESG), command and control information systems and ADP systems.

Chairman : Equipment Capability Manager

g. STANOC and Electronic Warfare Grading Sub-Committee (STEWGS) - with responsibility for surveillance, target acquisition, night observation, survey, counter surveillance, electronic warfare and directed energy weapons.

Chairman : Equipment Capability Manager

h. IS and COIN Grading Sub-Committee (ISCGS) - with responsibility for IS and COIN equipment, Special Forces and EOD.

Chairman : Equipment Capability Manager

Note : In each case, the secretary is provided from the Branch which supplies the Chairman. The results are published in the Army List of Classified Equipment (ALCE), edited by Def Sys ESB (OM).

3. Air Equipment Security Committee

Executive Secretary : DDef Sy(S&T)

This Committee does not meet formally. Its Executive Secretary, DDef Sy (S&T), obtains and disseminates the classification policies in major international collaborative projects, and through the Air Equipment Security Sub-Committees.

The Air Equipment Security Sub-Committees cover the following aspects of air equipment:

Aircraft and aircraft engines
Aircraft and ground equipment
Aircraft instruments
Air armaments and weapons
Avionics and electronics

Technical Secretariat for all the Air Equipment Security Sub-Committees is Def Sy (S&T).

These sub-committees meet at the relevant stage in the project when material classification changes are required.

Def Sy (S&T) are also responsible for the provision of classification guides for private venture funded equipment, atomic weapons and nuclear warheads, and guided weapons for all three Services.

4. Special Armour Security Committee (SASC)

Chairman : Equipment Capability Manager

This page intentionally left blank.

ANNEX U TO CHAPTER 12

SECURITY OF CONTRACTORS' PRIVATE VENTURE PROJECTS

1. 'Private Venture' (PV) projects are likely to fall within one of three categories:

   a. **Variants.** Variants of standard defence equipment under development or in production, eg aircraft, military vehicles or ships, etc with non-standard equipment or fitments, offered to meet special customer requirements or to avoid security or commercial difficulties associated with the sale of the Service item.

   b. **Derivatives.** Equipment for military or civil use which is not based on standard Service designs but depends on expertise or technology acquired in the course of defence contracts.

   c. **Freelance.** Equipment of defence importance which is in no way based on information gained from defence contracts.

2. IPT Leaders will be primarily concerned with variants or derivatives although cognizance may need to be taken of items in category (c) if they have an actual or potential military application. The Patent Office has arrangements whereby patents can be given security protection. (But see paragraph 12102d).

3. The variant is one of the more common forms of private venture. Many such variants may be no more than paper studies prepared for consideration by the defence department of other prospective overseas customers. Each variant should be subjected to a proper security assessment, since it may embody protectively marked aspects of Service projects and therefore require formal departmental approval of release before details of it may be made available to prospective overseas customers. Supporting documentation, etc may also require in-house protection by the contractor and by potential and actual customers.

4. The derivatives may not necessarily come formally to the notice of IPT Leaders. The existence of paper studies or work on such derivatives should in every case be reported to the security grading authority. A foreign power will rightly assume that Service technology is fully abreast of such derivative work, that the performance of Service equipment is unlikely to fall short of the performance of the derivative, and that there will be much in common in the design work. Hence a degree of security protection may be required to protect Service interests. Derivative projects may subsequently be adopted for limited or full UK Service use.

5. It is desirable that project managers be aware of the extent of contractors' obligations in respect of private venture work, since such obligations may not always be clear-cut and may be disputed. Both classified and unclassified defence contracts have clauses prohibiting the publication of material related to a contract without the approval of the department. In addition the Manual of Protective Security contains advice on reporting private venture work for grading (see paragraph 7 below). Contractors may have considerable commercial or other incentives for denying that their private ventures are in any way associated with Defence Contracts, though it is often possible to persuade them that the security protection of their own designs is not only in the public interest, but a factor of importance to prospective customers.

6. Overseas sales of private venture equipment need not concern IPT Leaders, **except** where they conflict with a contractor's undertakings to the department, eg if they make unacceptable demands on existing design, production, or testing resources, or where they require the release of information (protectively marked or unclassified).

7. For further information on private venture funded projects, see the Security In Industry insert B1 of the Manual of Protective Security.

ANNEX V TO CHAPTER 12

TEMPLATE OF SECURITY REQUIREMENTS (TSR) FOR CONTRACTORS REQUIRING ACCESS TO [INSERT NAME OF SITE]

Contents

TEMPLATE OF SECURITY REQUIREMENTS FOR CONTRACTORS REQUIRING ACCESS TO *[insert name of site]*

Introduction

1. **The information contained in this Template of Security Requirements (TSR) details the obligations and requirements of the Establishment Security Officer (ESyO) and Contractors when contractor personnel require access to *[insert name of site]*.**

Background

2. The Ministry of Defence (MOD) is subject to threats from espionage, sabotage, subversion, terrorism and crime, and has a security infrastructure throughout the Department. To counter these threats, the Department has established a range of security regulations and procedures with which the Contractor will be required to comply. Security is the responsibility of **all** personnel on MOD sites and contract (including sub-contract) employees are to comply with all security regulations and orders that are in issue (or may, from time to time, be issued) by the Head of Establishment or on his behalf by the Establishment Security Officer (ESyO) or other Security Authority. The Contractor is required to have a disciplinary system to ensure that action can be taken against any member of staff who fails to comply with security regulations or orders.

Guidance

3. The purpose of this TSR is to provide basic principles and guidance on the security requirements when contractors personnel are required to undertake work at ***[insert name of site].*** The policy and specific security regulations are contained in JSP 440 (Defence Manual of Security). In particular further information can be found in JSP 440, Volume 1, Chapter 5 on Physical Security and the requirements on Access to sites, Chapter 12 on Contract Security and Vetting of contractor personnel in Volume 2. Copies of this TSR must be provided to the Contractor's Site Manager or his deputy as appropriate for communication to the contractors personnel.

4. One of the main activities of security is to control access, which includes the reception of visitors. One of the purposes of access control is to establish identity, especially that of temporary or short term contractors, for whom it may not be practicable to carry out security vetting (which may involve Counter Terrorist Check (CTC) clearances) which takes up to 6 weeks, or 6 months for the higher or foreign clearances. Access measures may involve vehicle and body searches and, very

importantly, the need to escort those not in possession of a Defence Identity Card or a local unescorted access pass. However, escorting is seldom possible without a detrimental effect on the efficient running of the unit, and the instructions in this TSR are designed to give flexibility whilst maintaining security. For instance, it may be reasonable to accept that the identity documents provided by recognised organisations to their employees towards proof of identity. Also the new Driving Licence with photo is likely to be accepted.

Reporting requirements and security meetings

5. At the request of the ***[INSERT NAME OF SITE*** Designated Officer (DO), the Contractor's Site Manager is to report directly to the ESyO on the status and effectiveness of the security and service provided. All suspected security incidents and breaches of security are to be reported, in the first instance, to the ESyO. Records of such incidents are to be maintained by both parties. However, the DO retains primacy over all security-related matters on behalf of the HOE.

6. The Contractor's Site Manager, or his deputy, is required to attend unit Security Committee meetings to review and, if necessary, amend security practices in line with Government or MOD requirements. In addition, the Contractor's Site Manager is to nominate employees of a management/supervisory level from each of the main functional areas operated by the Contractor to perform the role of Contractor Security Office (CSO). The CSO will also be required to attend Security Committee meetings.

Nominated security officials

7. The nominated security officials for ***[insert name of site]*** and ***[insert name of company]*** are:

For ***[insert name of site]***

Insert details of post and post holders name

For ***[insert name of company]***

Insert details of post and post holders name

Definitions and abbreviations

8. The definitions and abbreviations applicable to this TSR are contained in Appendix 1.

Reference documents

9. The references applicable to this TSR are contained in Appendix 2.

Personnel security

10. A fundamental part of personnel security within the MOD is the principle that access to classified or protectively marked material is limited to those personnel with the need to know the information in order to perform their duties efficiently. This is known as the "need to know" principle and is enforced irrespective of rank or appointment.

11. In addition to the need to know principle, access to classified material is not permitted unless the appropriate security clearance has been granted. The process leading to the issue of a security clearance is called security vetting. The Contractor is to ensure that all staff are subjected to background checks. All posts filled or created by the contractor are to have the appropriate level of clearance determined by the level of access given on a case by case basis. In addition, where access to national caveats is concerned, the rules in JSP 440 Volume 1 are to be applied. Where necessary, the ESyO will advise on the level of security clearance needed subject to the level of access required.

12. The policy on security clearances for the MOD is contained in JSP 440 Volume 2. The minimum level of clearance for any contract employee to have unescorted access to MOD sites is the Basic Check (BC), in addition, a CTC is needed for all who declare Irish or certain foreign connections. CTC may be needed for all employees at sites of special importance, or where criminal convictions have been declared or are suspected. All contractor employees are required to fill in the Security Questionnaire MOD Form 1109 which will be checked by the ESyO, or completed under his supervision. The BC is an employment check and may also be carried out by the contractor under the supervision of the ESyO. This level of clearance also permits supervised access to assets upto and including those protectively marked CONFIDENTIAL. Any access to SECRET material requires Security Check (SC) clearance, and access to specific higher levels, such as regular access to TOP SECRET requires Developed Vetting (DV). Dual nationals (of which one nationality is British) may only have access to UK EYES DISCRETION information with the approval of the originators. If the contract involves the release of UK EYES DISCRETION information to named recipients, such individuals may only exercise their named recipient discretion, to disseminate further, in consultation

with the originator or owner of the information. The ESyO will provide advice on which posts need to be DV-annotated. There may also be access restrictions to some types of protectively marked material by people who hold another nationality in addition to British or who are not entirely British nationals.

13. No contract employee engaged to fill a post requiring a security clearance shall be granted access to protectively marked material until the ESyO has proof of the clearance being granted. Vetting can be a lengthy process. The average time taken for the most common checks and clearances are: BC, which requires proof of identity and 2 references a day or 2; CTC, after BC is complete, 6 weeks from submission, but may take up to 6 months if a foreign country is involved; SC up to 6 weeks; DV up to 6 months. Currently, MOD does not charge for vetting, but the Department reserves the right to introduce such charges.

14. In all instances, BC procedures are to be completed by the Contractor and the results notified to ESyO, in the form of a Basic Check Verification Record (BCVR), in advance of personnel reporting for work. If the Contractor is a List X firm, and personnel have already been security cleared, it is the firm's responsibility to notify the EsyO of the security clearance details of the personnel. Clearance levels of such personnel are to be notified to the ESyO before access to protectively marked material will be granted. If the Contractor is either not a List X firm or is a List X firm but the personnel do not hold the relevant clearance, it is their responsibility to ensure that vetting applications are completed, in respect of their own and any Sub-Contractor's staff, and submitted to the ESyO who, after verifying that clearance is required, will formally sponsor the clearance application and forward the forms to the appropriate Vetting Authority.

15. The Contractor is required to maintain a current list of all employees, Sub-Contractors and their agents detailing all posts, requisite security clearance levels and expiry date, along with the personal details of the incumbent and provide the ESyO with an updated list upon request. The Contractor is responsible for maintaining an auditable and accurate record of the security clearance of all personnel introduced to the establishment in conjunction with the contract, for a period of 7 years. Should any circumstances arise which could bring into question an employee's suitability to hold or retain security clearance, or to have continued access to ***[insert name of site]***, the Contractor is required to notify the ESyO without delay.

16. No contract employee shall be allowed unescorted entry to ***[insert name of site]*** without BC, and CTC when needed, unless specifically authorised by the ESyO. However, contractor employees holding full passes may be authorised by the ESyO to escort other employees awaiting CTC or SC. Apart from this, these checks are the minimum necessary for employment within, and to permit unescorted access to, ***[insert name of site]***. Access to assets protectively marked SECRET or above is not permitted unless the appropriate level of security clearance has been granted.

17. Under Government nationality rules, the MOD can refuse to disclose or permit access to information if disclosure or access would be contrary to the national security interest. In particular, material bearing certain caveats carries nationality qualifications.

Physical security

18. The ESyO is responsible for determining the physical security measures appropriate for the safeguarding of protectively marked material. The type of secure container, lock and level of checking required will be assessed and instructions issued in accordance with security regulations.

19. Contractors and their staff will be required to adhere to the MOD policies on physical security and be responsible for the handling and storage of sensitive materials, data and information in their custody or control. Security containers will be provided. All protectively marked material is to be handled in accordance with JSP 440 Volume 1.

Counter Terrorism

20. The overall responsibility for counter terrorism (CT) within the UK lies with the civil police. At ***[insert name of site]*** the is ESyO responsible for actioning CT measures for the protection of personnel within MOD property. It is the responsibility of the Contractor, Sub-Contractors and their staff to cooperate with any security measures that may be imposed. Any staff who fail to comply with CT measures increase the risks to all personnel and will be liable to be excluded from ***[insert name of site]*** either permanently or for a prescribed period at the discretion of the ESyO.

Security access

21. Access to ***[insert name of site]*** is the prerogative of the Head of Establishment who has the authority to exclude personnel or their vehicles from MOD property in response to security threats or personal indiscipline.

22. The ESyO is responsible for enforcing access control policies, and the Contractor is responsible for ensuring that all staff comply with control of entry requirements. All persons entering ***[insert name of site]***are required to positively identify themselves and are liable to be searched on entering or leaving the Establishment and at certain other facilities. Failure to comply may render staff liable to exclusion from the Establishment.

23. All contract staff are to be in possession of a Pass at all times within the bounds of ***[insert name of site]***. In addition, all staff are expected to identify

themselves using the Pass, upon the request of any Service person or other MOD employee.

24. The ESyO is responsible for issuing all contract personnel with a Pass. The Contractor is responsible for ensuring passes are withdrawn from those personnel who leave his (or his Sub-Contractor's) employ, and returned to the ESyO for cancellation.

25. Physical access to areas holding official or protectively marked information (in whatever form) may need to be restricted. In particular:

a. The DO retains the right of access to the Contractor's premises, as well as to any information stored on systems, and the information held by the Contractor or his Sub-Contractors. For example access by the Establishment's security staff, MOD security auditors, the Data Protection Registrar and the National Audit Office carrying out security monitoring, spot checks etc.

b. The Contractor, his Sub-Contractors and their agents will be granted any necessary access to the Establishment for maintenance or inspection purposes, providing the ESyO is informed and the individuals meet the necessary security criteria.

c. The DO retains the right to implement security spot checks on all the Contractor's staff and security records and, either in isolation or in conjunction with the Contractor, his Sub-Contractors or agents.

d. The Contractor is to ensure that all staff are made aware of the "need to know" principle and is to limit access to protectively marked assets to those who require such access in the course of their duties. Further advice regarding access restrictions may be obtained from the ESyO.

International arms inspections

26. ***[insert name of site]*** may be tasked to abide by international treaties in order to facilitate verification of various arms and/or weapons limitation or reduction agreements. The scope of these inspections is detailed in respective Operation Orders. All contract employees, including Sub-Contractors and their agents, are to ensure they do not obstruct these inspections and must be meticulous regarding the release of information (Appendix 4, Serial 8 refers).

Security operations

27. There are a number of counter-terrorist measures, which may be implemented at short notice or over extended periods, intended to protect from, or at least diminish the effects of, various terrorist threats against the Establishment and its personnel. These include operations BIKINI, TESSERAL and ROUNDUP as well as other contingency plans. Specific details and required responses are detailed in security Standing Orders.

Security of Information Technology (IT) systems

28. The introduction and use of IT hardware and software to ***[insert name of site]*** is to be strictly controlled in accordance with JSP 440 Volume 3 and local security Security Orders. No hardware or software is to be introduced or used on the Establishment until it has been registered with the EsyO, accredited and virus-checked. The DO retains the right of access, audit and ownership of all official and protectively-marked information stored or processed on IT controlled by the Contractor, his Sub-Contractors and their agents. There are strict security rules governing the interconnection of IT systems and approval must be sought from the ESyO prior to any connection/alteration being made to any network or system.

29. The Contractor is expected to cooperate with IT protection programmes that may entail MOD Computer Security staff having access to the Contractor's IT equipment. The Contractor should be aware that his own 'Commercial' information will be accessible by MOD Computer Security staff conducting such duties and should give due consideration to storage of his information on site.

Communications discipline and security

30. The Contractor is to ensure that employees comply with the requirements of JSP 440 and security Standing Orders prior to using any electronic communications system at ***[insert name of site]***. The use of mobile/portable telephones, CB radios and other telecommunication equipment on ***[insert name of site]*** is restricted and their use is to be strictly in compliance with JSP 440 and security Standing Orders.

Approved security products

31. Many security products and systems have been evaluated and/or certified by Government Authorities, eg for IT through the IT Security Evaluation and Certification Scheme, for physical security by the Evaluation and Development in Counter Terrorism and Sabotage (EDICTS), and for equipment approved by the Security Equipment Advisory Panel.

32 The use of approved security products falls into 2 categories: those to which the Contractor will have access, and those installed by the Contractor. Should a Contractor have access to, or custody to, approved security products, he should be aware that any unauthorised disclosure of information regarding any aspect of the product may constitute a breach of the Official Secrets Acts and Copyright law.

33. The ESyO 's consent is required prior to the introduction or use of any non-approved equipment. This includes the use of any 'innovation' developed by the Contractor.

Crime Prevention

34 The Contractor is to establish an internal control programme to eliminate fraud and theft. The Contractor's employees will be expected to cooperate with MOD policy crime prevention programmes, which include submitting to a cursory search of vehicles and bags entering and leaving ***[insert name of site]***.

Training

35. With assistance from the ESyO the Contractor is required to train his staff, and those of his permanent Sub-Contractors or agents, to a level of competence and understanding of security regulations that will enable them to ensure they are complied with at all times. Indeed, all personnel are to receive security training to the level and within the timescale detailed in Appendix 3. The course content for all security training is to be agreed by the ESyO.

36. General security education and problem-solving advice on security matters is to be provided by the ESyO.

TSR schedule

37. A TSR Schedule is at Appendix 4 for the guidance of Security Staff and should be included in the TSR, though adapted for each situation.

Appendices:

1. Definitions and Abbreviations.
2. Reference Documents.
3. Security Training Requirements.
4. TSR Schedule

APPENDIX 1 TO ANNEX V

DEFINITIONS AND ABBREVIATIONS

Serial No	Term, Expression or Title	Definition
(a)	(b)	(c)
1	Establishment Security Officer (ESyO)	ESyO is the generic term for Base Security Officer (BSO) or Unit Security Officer (USO) in the Royal Navy, Unit Security Officer (USO) or Branch Security Officer (BSO) in the Army, Station Security Officer (SSyO) in the Royal Air Force and the appointed chief specialist security officer in MOD Agencies or industry.
2	Designated Officer	The person to whom the HOE has delegated authority for the routine supervision and monitoring of requirements incumbent upon contractors requiring access to a specific site.
3	Contractor Security Officer (SO)	The Contractor's appointed employee responsible to the ESyO for the implementation of security policy and procedures within his specified area of responsibility.
4	Personnel Security	Personnel Security is the principle that access to protectively marked material is not permitted unless an appropriate security clearance is in issue. This process is called vetting.
5	Security Vetting	The Basic Check is needed for security vetting and CTC clearance and, whilst not in itself a vetting measure, allows authorised and supervised access to CONFIDENTIAL on a need to know basis. Vetting includes Security Check (SC) for SECRET, Developed Vetting (DV) for higher access and Counter Terrorist Check for those with Irish or some foreign connections and some others.

6	Need to Know	The "Need to Know" principle ensures that access to protectively marked material is limited to those personnel who need to know the information in order to carry out their duties efficiently. This "need to know" principle is enforced regardless of rank/status or appointment.
7	Protective Security	The MOD protects its assets in terms of the threat posed and the value of the material. A protective marking indicates the value of material. Material with a protective marking is to be safeguarded in accordance with security regulations.
8	Protective Marking	A protective marking is given in accordance with an assessment of the damage that would be caused in the event of material being disclosed to unauthorised persons. The levels of protective marking (in ascending order) are RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET.
9	Caveat	A caveat is an additional marking applied to material that is subject to special handling requirements in addition to those procedures required by its protective marking. Eg UK EYES ONLY
10	Descriptor	A descriptor is a caveat added to a protective marking indicating the subject being covered. The use of the descriptor further restricts access to a document beyond that normally imposed by vetting requirements. Eg MEDICAL
11	Proof of Identity	Acceptable documents are those listed in JSP 440, Volume 2 .
12	Positive Identification	The confirmation of an individual's identity by means of either visual recognition or approved proof of identity.

13	Pass/Identity Card (Not temporary)	A card of an agreed design bearing a clear full face (or front ¾ face) photograph of the bearer along with their basic personal details in a clear point face.
14	MDP	Ministry of Defence Police.
15	SGF	Security Guard Force.
16	MGS	Ministry of Defence Guard Service.
17	MPGS	Military Provost Guard Service
18	JSP	Joint Services Publication.
19	List X	Term given to a contractor's site that is required to hold protectively marked material CONFIDENTIAL or above. A list X site will have a security controller security oversight and inspection is undertaken by the Security Service acting on behalf of D Def Sy

This page intentionally left blank.

APPENDIX 2 TO ANNEX V

REFERENCE DOCUMENTS

Ser	Publication Reference	Title	Remarks	M or G
(a)	(b)	(c)	(d)	(e)
1	DMS (JSP 440) Vols 1-4	Defence Manual of Security	MOD Security Regulations	M
2	MPS	Manual of Protective Security	Baseline Security Manual issued by the Cabinet Office and used by List X sites and by Government Departments who may devise more stringent regulations	M/G
3	DMS Vol 1 Chap 16	Regulations for the Use of National Caveats, The Caveat "LOCSEN" and the Special Marking "UK Comms Only"		M
4		Manual of Personnel Administration Volume 1	Contains Registry procedures	M
5	OSA	Official Secrets Acts (1911-1989)		M
6		Local Standing Orders		M
7		Local Standing Orders (Security)		M

The notations against the above references have the following meanings:

M - Adherence to the policies and procedures contained therein is mandatory.

G - The policies and procedures contained therein are not mandatory, but proposals for alternatives must fully interface with procedures in use globally.

This page intentionally left blank

APPENDIX 3 TO ANNEX V

SECURITY TRAINING REQUIREMENTS

Serial No	Post/Functional Area	Training	Frequency	Remarks
(a)	(b)	(c)	(d)	(e)
1	Managerial Post Holders	Induction - ½ Day	On Appointment	Within one month of taking up appointment.
2		Handling protectively marked material - ½ day	On Appointment	Within one month of taking up appointment.
3	All ESyOs	ESyOs course - 3 days	On Appointment	Within 3 months of taking up appointment.
4	All Registry/Typing/ Admin Staff	Registry Course - 5 days	On Appointment	Within one month of taking up appointment.
		S&C Course - 2 days	On Appointment	Within one month of taking up appointment.
5	IT Installation Managers	Installation Managers Security Course - 3 days	On Appointment	Within one month of taking up appointment.
6	All Staff	Induction - ½ day	On Appointment	Within one month of taking up appointment.
		Refresher - up to ½ day	Annually	Within 12 months of any previous induction or refresher course.

Note:
This table is representative and may require extension or modification to take account of posts at individual establishments.

This page intentionally left blank

APPENDIX 4 TO ANNEX V

TSR Schedule

Item No	Major Contract Requirement	Related Requirement or Information	Performance Standard
1	**General**		
1a	Attend Establishment Security Committee meetings to review and, if necessary, amend security practices in line with MOD, Service or Authority requirement.	The Contract Manager or Deputy is to attend Establishment Security Committee meetings.	No instance of failing to attend meetings.
1b	Nominate employees of management/supervisory level from each of the functional areas operated by the Contractor to perform the role of Contractor SO.	Contractor USOs are to attend Establishment Security Committee meetings.	No instance of nominated Contractor SOs failing to attend meetings.
1c	Report all suspected and actual security incidents and breaches of security to the ESyO.	Additionally, at the request of the DO, the Contractor's Site Manager is to report directly to the DO on the status and effectiveness of the security of the service provided by the Contractor.	No incidence of failing to report suspected and actual security incidents and breaches of security within 24hrs of event or sooner if situation demands.
2	**Security Clearances**		
2a	Ensure all contract staff are subject to background checks and vetting as required.	No staff will be permitted unescorted access to MOD property until a CTC screening has been satisfactorily completed.	No uncleared staff on site.
2b	Ensure Contract manager and any Deputy(ies) are cleared to the appropriate level.	If access to protectively marked material is required in connection with contract performance.	No uncleared contract management staff employed on the project.

Item No	Major Contract Requirement	Related Requirement or Information	Performance Standard
2c	Ensure all relevant post holders are cleared to respective level.	Access to protectively marked material and/or a war planning role.	No uncleared staff in post**.**
3	**Vetting Administration Requirements**		
3a	List X Contractors		
3a(i)	Conduct BC in respect of all contract employees (including Sub-Contractor employees).	Clearance and checking procedures in accordance with Cabinet Office Manual of Protective Security.	100% of BC action conducted by the Contractor.
3a(ii)	Notify the ESyO of the clearance level of any staff previously cleared under the List X system, before they report to work.	SC/DV is to be in issue before any access to protectively marked material connected to annotated posts can be permitted.	No more than 25% of clearances notified <48hrs and >24hrs before starting work. No clearances notified <24hrs before starting work.
3b	Non-List X Firms		
3b(i)	Conduct all BC action in respect of all directly employed and sub-contracted staff.	Checking procedures in accordance with Cabinet Office Manual of Protective Security.	100% of applicants to have BC action completed by the Contractor.
3b(ii)	Ensure that prospective staff, including Sub-Contractors' staff, complete vetting forms as required by ESyO.	Failure to satisfactorily complete vetting forms could result in staff being denied access to a Project site.	No incidence of contract (including sub-contract) staff requiring access to a Project site before CTC or vetting is completed.
3b(iii)	When required, ensure that all completed CTC forms are submitted to the ESyO for processing.	The ESyO is responsible for conducting CTC screening and for processing other security clearance applications to DVA.	Not more than 20% submitted <72hrs but >48hrs and 10% submitted <48hrs but >24hrs, before access required.

Item No	Major Contract Requirement	Related Requirement or Information	Performance Standard
4	**"Need To Know" Requirements**		
4a	**Maintain the"need to know" principle at all times.**	No person is entitled, by virtue of rank or appointment, to have knowledge of or possession of protectively marked material unless they have a "need to know" in order to discharge their duties efficiently.	No incidence of staff of the Contractor, his Sub-Contractors and their agents failing to maintain the "need to know" principle.
5	**Protective Security**		
5a	Safeguard protectively marked material in accordance with security regulations.	Security standards determined by the Easy based upon policy laid down set out in JSP 440 Vol. 1.	No incidence of protectively marked material improperly safeguarded**.**
5b	Secure protectively marked material when not in use.	In accordance with standards laid down by the Easy.	No incidence of protectively marked material not properly secured when not in use.
5c	Administer protectively marked material in accordance with regulations.	In accordance with JSP 440 Vol. 1 and any appropriate single Service publications.	No incidence of protectively marked material inadequately administered.
6	**Counter Terrorism**		
6a	Comply with CT measures.	Measures will be set out by the Easy and will vary according to the threat level.	No incidence of contract (including sub-contract) staff failing to comply fully with CT measures.
7	**Access Requirements**		
7a	Show Pass on demand.	Pass to be issued by the ESyO.	No incidence of contract (including sub-contract) staff failing to identify themselves on demand by means of a Pass.
7b	Submit to searches of vehicles, bags, packages and clothing on demand.	Searches will be conducted in accordance with strict policy guidelines.	No incidence of contract (including sub-contract) staff failing to submit to a cursory search on demand.
7c	Ensure that all contract staff are in possession of a Pass before starting work.	Pass to be withdrawn on completion of employment at a Project site or on termination of employment with the Contractor.	100% of contract (including sub-contract) staff issued with a Pass.

Item No	Major Contract Requirement	Related Requirement or Information	Performance Standard
7d	Carry a Pass at all times within the bounds of MOD property.	Pass to be produced on demand.	No incidence of contract (including sub-contract) staff failing to carry Passes at all times.
7e	Display a valid vehicle pass in all Contractor's and staff owned vehicles within MOD property.	Passes issued by ESyO Pass Office.	No incidence of vehicles belonging to the Contractor, his Sub-Contractor, their agents and their staffs not having a vehicle pass on display whilst on the Unit.
7f	Withdraw and return all MOD issued passes and permits from contract (including sub-contract) employees who no longer require or are no longer permitted to enter MOD property.	Passes to be returned to ESyO or Pass Office.	No incidence of contractor (including sub-contract) employees, or former employees, retaining Passes and permits to which they are no longer entitled.
7g	Permit right of access to Contractor's premises, to any information stored on systems and to any information held by the Contractor, Sub-Contractor or contract employee.	Access by DO and official staff only, eg. Establishment security staff, MOD security auditors, the Data Protection Registrar, National Audit Office carrying out security monitoring, spot checks etc.	No incidence of Contractor's, his Sub-Contractor's and their agents' staff denying access to DO or official staff.
8	**International Arms Inspections and Security Operations**		
8a	Ensure that all contract staff do not obstruct International Arms Inspections.	Actions and associated measures detailed in Operation Orders and Security Standing Orders.	No incidence of contract (including sub-contract) staff obstructing Arms Inspections.
8b	Be meticulous in the release of information during International Arms Inspections.	Guidance detailed in Operational Orders.	No incidence of contract (or sub-contract) staff releasing gratuitous information.

Item No	Major Contract Requirement	Related Requirement or Information	Performance Standard
9	**Security Requirements**		
9a	Register all IT hardware and software introduced or used on the Establishment.	Register held by ESyO.	No incidence of unregistered IT hardware and software being introduced or used on the Establishment.
9b	Control and administer all IT systems and their associated media used to process official information.	In accordance with JSP 440 and Security Standing Orders.	100% compliance with MOD regulations.
10	**Communications Discipline and Security**		
10a	Comply with Communications Discipline and Security requirements.	In accordance with JSP 440 and Security Standing Orders.	No incidence of contract (including sub-contract) staff failing to comply fully with Communications Discipline and Security requirements.
11	**Security Approved Products**		
11a	Maintain the integrity of approved security products.	Any disclosure of information relating to approved security products could be in breach of Official Secrets Act and/or copyright law.	No incidence of contract (including sub-contract) staff disclosing any information relating to approved security products.
11b	Obtain the ESyO's consent before initiating any innovation.	The ESyO will determine if the use of security approved products is required.	No incidence of non-security approved products being used without the agreement of the ESyO.
12	**Crime Prevention**		
12a	Establish internal control programme to eliminate fraud and theft.	Programme shall include periodic policing of Contractor's controlled facilities to detect pilfered goods. Full co-operation with ESyO, MGS, MDP and other security representatives as required.	No pilfered goods found in Contractor's controlled facilities as a result of Contractor's failure to conduct inspections.

Item No	Major Contract Requirement	Related Requirement or Information	Performance Standard
13	**Training Requirements**		
13a	Attend induction and refresher security training.	As set out in Appendix 3. Course content agreed by the ESyO.	100% attendance at courses within prescribed timescales.
13b	Attend security training relevant to posts involved in handling protectively marked material.	As set out in Appendix 3. Course content agreed by the ESyO.	No incidence of untrained personnel handling or having access to protectively marked material unsupervised.
14	**Records and Deliverables**		
14a	Maintain records on the creation, copying, registering, movement, transmission or destruction of protectively marked material in accordance with Government, MOD and any Service regulations.	In accordance with JSP 440 Vol 1 and Security Standing Orders.	No incidence of incorrectly maintained records.
15	**Materials, Equipment and Facilities**		
15a	Registers, charging sheets and other forms and documents required to administer protectively marked material will be available through the stationery supply system.	As required by JSP 440 Vol 1 and Security Standing Orders.	No incidence of incorrect forms being used in the administration of protectively marked material.

Item No	Major Contract Requirement	Related Requirement or Information	Performance Standard
16	**Government Furnished Equipment**		
16a	Security Locks and Furniture. Approved security locks and furniture will be supplied through the supply system.	As required by JSP 440 Vol 1 and ordered through the ESyO.	No incidence of protectively marked material being stored in anything other than approved security furniture.

This page intentionally left blank.

CHAPTER 13

SECURITY EDUCATION, TRAINING AND AWARENESS

This page intentionally left blank.

CHAPTER 13

SECURITY EDUCATION, TRAINING AND AWARENESS

Introduction

1301. General. Security education and training are important command/management responsibilities at all levels. The threat from overseas intelligence services and terrorist organizations is considerable; and the consequences of poor security in MOD establishment could be disastrous. The best precaution against lapses in security is to ensure that everyone is properly trained.

1302. Aims. This chapter covers two aspects of one subject, the aims of each are:

a. **Security education**. To ensure that all who work within the MOD, both military and civilian, irrespective of their access to protectively marked assets/material, understand both the security threat and their responsibilities for countering it.

b. **Security training**. To ensure that those individuals who have specific security responsibilities as part of their normal employment are properly trained in their security duties.

1303. Higher coordination. This is achieved by means of the Security Awareness Working Group (SAWG) which is chaired by DDefSy.

Responsibilities

1304. The Ministry of Defence. The Director of Defence Security (DDefSy) is, inter alia, responsible for formulating and sustaining policy on, and coordination of, security education and training in the MOD as a whole.

1305. Central Budget Security (HQ, PE & Industry). CB(Sy) is responsible for advising on security training requirements throughout the MOD civilian estate. It includes a small training branch for the provision of basic protective security training and Branch Security Officer (BSO) courses and liaises with other agencies to facilitate more specialised training.

1306. The Defence Intelligence and Security Centre (DISC). DISC is a Defence Agency and is located at Chicksands. It comprises the following schools:

a. Defence Intelligence and Security School (DISS)

b. Joint School of Photographic Interpretation (JSPI)

c. Joint Service Intelligence Organisation (JSIO)

d. Defence Special Signal School (DSSS)

The Chief Executive of the School is responsible to 2SL/CINCNAVHOME and to CinC LAND, inter alia, for:

e. Advising DDefSy through the Services security training HQ about security education and training;

f. Implementing Royal Navy and Army security training policy through courses of instruction at, or sponsored by, the DISC.

1307. The RAF Provost & Security Training Squadron (P&STS). P&STS is located at RAF Halton. The OC is responsible for implementing Royal Air Force security training policy through courses of instruction at P&STS.

1308. Heads of Service Security. These are responsibilities for:

a. Ensuring that officers and Service personnel are nominated by heads of establishment to attend relevant courses at DISC/P&STS, as appropriate. The courses should be attended preferably before, but always as soon as possible after, taking up appointments involving security duties.

b. Organizing the security training of those establishment security officers (ESyOs) and establishment IT security officers (EITSyOs) who have not attended courses at DISC/P&STS; and that of senior secretarial staff.

c. Providing advice and assistance for both intermediate level and establishment security education and training.

d. The preparation and issue to DISC and to P&STS and down the chain of command of education and training material from case histories and reports.

e. Monitoring security education and training in establishments by means of security inspections.

1309. Intermediate Commanders. These commanders are responsible for the security education and training within their command. Such commanders can make a major

contribution to security training by demanding high standards of security alertness at all times, whether in peacetime stations, during training, on exercises, or on operations. Security education and training will normally be commented on as part of the annual report on a vessel or establishment.

1310. Directors and heads of divisions in MOD and MOD agencies. Such persons are responsible for ensuring that:

a. All staff receive security education on initial recruitment, and periodically thereafter, so that they are fully aware of the security threat and general counter measures.

b. All staff who handle protectively marked documents/material or equipment receive security training relating to their responsibilities, and that the training is periodically updated.

c. Those personnel who have full or part-time security duties attend suitable education and training courses to enable them to fulfil their responsibilities.

d. The organisation and management of security education and training within their respective establishments is in accordance with MOD policy.

1311. Heads of establishments (HOE). These individuals are the most important links in the chain of command/management as far as security is concerned. It is therefore imperative that such persons should be, and be seen to be, thoroughly security conscious; they must insist on the highest standards of security throughout the establishment. They must appoint an ESyO and an EITSyO and make sure that they are properly trained by attending the appropriate course(s) prior to taking up their appointment, or within three months of doing so. The single most important factor in maintaining high standards of security will be the attitude adopted by the head of establishment to this subject.

1312. Establishment security officers (ESyO). The generic responsibilities of the ESyO are shown at para 0227 in Chapter 2 of Volume 1; and those of the EITSyO are given in Annex B to Chapter 1 of Volume 3.

1313. The ESyO, in conjunction with the EITSyO, should organize and arrange for security education and training on behalf of his HOE; so that all personnel understand the nature of the threat to security, and are instructed in the application of security procedures to counter the threat. Security education and training should be a continuous process; it must never be allowed to recede into the background due to other pressures. Special attention must be given to ensure the appropriate training of all personnel whose employment involves security duties. Such personnel include:

a. All officers, warrant officers and senior non-commissioned officers, with particular reference to such duties as orderly officers, guard commander, etc.

b. Clerks, secretaries and all those who handle protectively marked documents.

c. Engineers, technicians, arms/ammunition/explosives storemen, armourers, and others responsible for protectively marked equipment.

d. Service and unit police, members of unit guards including civilian security officers (MOD Guard Service) and contract guards.

e. Post orderlies and messengers.

f. Radio, telephone, facsimile and teleprinter operators.

g. Computer operations and users.

1314-1320. Reserved

Security education

1321. The security education needs of new recruits should be assessed and met as early as possible. Security education should be part of an ongoing training process, to ensure that the subject is not allowed to lapse into the background. Properly handled, security education should make all members of the Armed Services and all civilians who work for them or for the MOD aware:

a. That a threat exists and its nature (see para 1322 below).

b. That the individual has personal responsibility for security including their own.

c. Of the relevance of protective security measures.

d. Of the need for good security at all times.

e. Of the security risks associated with overseas travel, more especially for those with SC and particularly with the DV clearances.

1322. The Threat. Current threats to security, not in any particular order of priority, arise from:

a. Espionage, including commercial espionage.

b. Sabotage.

c. Subversion.

d. Terrorism.

e. Non traditional threats, eg leakage, hacking, fraud theft and criminal damage.

Full details may be found in **Chapter 1**.

1323. Weapons, ammunition and explosives. All serving personnel are to be regularly reminded to pay the greatest attention to the security of weapons, ammunition and explosives (see Chapter 6). The need for maximum vigilance in this matter is underscored by the fact that such items stolen from the military are known to have been used to murder British servicemen.

1324. Annual Refresher Education.

a. All staff must be given security education at least once in a calendar year. The subjects to be covered are non-exhaustive but must include topics listed in para 1321 above.

b. ESyOs are to maintain the following in a dedicated register:

(1) Names of personnel attending.

(2) Topics covered.

(3) Place, time and date.

(4) Type of security education given, eg formal presentation, written brief, post incident de-brief, annual confidential orders, routing orders/instructions or other medium as appropriate.

c. This register is to be produced on request during inspections/investigations.

1325. Reserved.

1326. Teaching. Security education can be dull, unless it is put over imaginatively and in a way that grips the interest. The aids which should be considered are detailed at Annex B.

1327. Internal security education material. Internal security education material will be coordinated where necessary by DDefSy and includes:-

a. **Desk calendars and other devices bearing security messages**. Desk calendars and other devices bearing security messages whose aim is to remind staff of their personal responsibility for security, particularly for those procedures most closely related to desk work: locking away protectively marked documents, ensuring that assets receive the proper protective markings, etc.

b. **Publications, staff circulars and newsletters**. Publications, staff circulars and newsletters which may be used for:

(1) Promulgating security regulations and amendments.

(2) Relating instances of breaches of security and the lessons to be learnt from them.

(3) Encouraging the avoidance of breaches, perhaps by periodic circulation of statistics within a department - which might serve as a way of promoting a sense of competition between branches, sections and divisions to achieve the highest security standards.

(4) Warning staff of specific or topical threats to security and providing guidance in countering them.

(5) Providing a channel or communication with staff on security matters generally.

1328. External security education material. The quarterly "Security Education News" (SEN) and other occasional briefing notes, booklets and pamphlets published by the Security Service contain topical and timely articles and advice on security issues. Whenever possible, SEN uses Clip Art illustrations. Persons controlling security education may use and reproduce this material to promote security as an integral part of the work of the individual and organisation.

1329. New procedures. When changes in security rules or procedures are introduced, care is to be taken to ensure that these changes are made known to those affected. Furthermore, any fresh training that may become necessary as a result of such changes should be conducted without delay.

1330-1339. *Reserved.*

Security training

1340. Such training is mandatory for all officers and civilians going to security staff appointments, including those where security is only part of their work. It is also necessary for all types of establishment security officer, secretarial staff, those engaged with weapons or explosive ordnance, and all others whose duties impinge on, or have an element of security in, their responsibilities. The appropriate Director of Security or his equivalent lays down the type of course that all staff officers and civilians with security responsibilities should attend. All lead command headquarters have this information.

1341. Range of subjects. Security training must invariably include instruction on:

a. The current threat.

b. Protective Security Principles - eg need to know, need to hold, defence in depth etc.

c. Good security practice and procedures, to embrace:

(1) Correct use of protective markings and descriptions;

(2) Physical, personnel, information, communications and information technology (IT) security.

d. An understanding that the compromise of assets encompasses unauthorised disclosure, interference (eg the amendment of a database), withholding (eg preventing Government from having access to the asset when needed, including through theft) or destruction.

e. Practical experience in applying the security rules and procedures on the tasks in which staff are, or will be, engaged.

f. Action to be taken if a breach of security is suspected (apart from reporting procedure, which will be confined to security staff and line management).

1342. Annual refresher training. The staff listed in Paragraph 1340 above are to receive annual refresher training. This training is to be recorded in a register, the details of which are specified in Paragraph 1324b(1) to (4). The subjects to be covered are primarily the **threat** followed by whatever topics listed in para 1341 above are most appropriate. Within Head Office establishments, responsibility for conducting this training rests with branch security officers. Outside Head Office, the training will be run by either security specialists or ESyOs.

1343. Training methods. Though a large amount of training will be through central courses of instruction; details of which are published annually in DCIs and by training teams visiting establishments, there will also be the need for talks and seminars. Detailed guidance is given in Annex B.

1344. External courses. The Ministry of Defence D Def Sy is able to arrange vacancies on outside courses of kinds not seen within the MOD (normally of one day's duration) with the Security Service. The Civil Service Staff College also runs a number of security courses, which are chargeable to local budget holders. Requests for further information and bids for vacancies should be made through Lead Commands, who hold details.

1345. Specialist training support. Both at home and in certain overseas commands Intelligence Corps and RAF P&SS personnel provide security education and training facilities for establishments within the commands. Elsewhere, specialist units provide

similar, but more limited, security education and training support as required by the security staff.

1346. IT security training. In addition to that available within the MOD, such training is also provided by the Security Service, the Civil Service Staff College, the Communications Electronics Security Group (CESG), DISC, P&STS and the Defence IT Management Training Centre (DITMTC). All these courses are open to both Services and civilian personnel.

Appointing, posting and promotion

1347. Individuals moving for the first time to posts with responsibilities and tasks involving protectively marked material should be fully briefed by the ESyO on the security implications of the work, and the correct practices to be adopted on taking up their positions. Whenever possible, security education & training should be an intrinsic part of the preparation of a new post.

1348. Persons who already have some experience of protectively marked material should receive specific training when they are given significant additional tasks or responsibilities. In particular, further training will be required on management training courses. This should include a clear security education and training element, clarifying the respective responsibilities of line and personnel management for the security of staff in their charge. Examples of additional security education and training requirements, which are likely to arise from changes in or extension of duties include:

a. Appointments/postings abroad involving more sensitive work, different procedures, or shift work to outstations remote from headquarters or entailing contact with the media and/or representational duties.

b. Promotions involving increased staff management and/or security duties.

c. The introduction of new technology.

1349. Overseas postings and deployment. When a vessel/unit moves to another country/region overseas, it is important that all personnel should be briefed on the local threat in their new station and on local security regulations as soon as possible after arrival. Units, both regular and reserve, going for short periods of training abroad (eg from the United Kingdom to Cyprus) should similarly be given a security briefing.

ANNEX A

SUBJECTS FOR SECURITY EDUCATION

1. The subjects listed below are intended as a guide to those responsible for security education within an establishment:

a. The general threat to security - Para 1322 above and Chapter 1.

b. The current local threat as assessed by the appropriate security staff.

c. Individual activities which have inherent security dangers, such as:

(1) Private correspondence.

(2) Travel to foreign countries, especially those to which special security regulations apply (CSSRA). DMS Volume 2, Chapter 21.

(3) Loose talk.

(4) Public disclosure of official information.

(5) Amateur radio, Citizen Band and INTERNET activities.

(6) Telephone and radio security.

(7) Displaying insignias, badges, stickers etc that advertise an individual's association with MOD.

d. The Official Secrets Acts and reminders of what they mean.

e. Briefings on the dangers of social approaches and 'talent spotting' by overseas intelligence services. DMS Volume 2, Chapter 21.

f. The need for responsible conduct to avoid the possibility of blackmail. Chapter 1.

g. The importance of reporting immediately all suspicious occurrences, to include weaknesses in security procedures or vulnerable behaviour apparent in colleagues. The means of doing this in complete confidence should be widely known.

h. The requirement for high standards of security in relation to protectively marked documents and equipment, and in the use of communications. Chapter 4, 5, 6 and 9.

2. Terrorist methods and the resultant common sense precautions to be adopted by all personnel. Chapter 7.

ANNEX B

SECURITY TRAINING: INSTRUCTIONAL AIDS

1. **Multimedia Learning**. This is **the** teaching method of the future; a full background to this new topic is set out in Annex D.

2. **Lessons**. Lessons may be drawn from recent security intelligence cases, security breaches and terrorist incidents. Such material is available from security staffs and should be disseminated rapidly. Lessons may also be drawn from security surveys and inspections.

3. **Videos**. These provide a particularly effective way of informing large numbers of staff about the various threats to security, and of making them aware of their security responsibilities. They can be used as visual aids during a course or be the main focus of a separate security session. A video should never be used in isolation, but must be set firmly in its security context by the presenter, otherwise the audience will be inclined to judge it solely on its entertainment value and so obtain little or no security benefit from it.

4. Showing a video should therefore always be preceded by a short introduction, describing its purpose and points to look out for. A discussion about the value of the video and the security lessons it highlights should follow. If guidance notes for the use of presenters are not provided with the video, the presenter should compile his own. The Joint Services military training film and video catalogue, issued by the British Defence Film Library (BDFL), includes security educational and instructional material, produced tri-Service, single Service or by the Security Service. Virtually all recent production has been in the form of videos. Commands are responsible for notifying the release of new videos that are not yet listed in the catalogue. Videos should be chosen that are appropriate to the audience (eg civilian audiences may not relate to one featuring uniformed characters), and it should be suited to the expertise and seniority of the audience.

5. **Posters**. Posters are not intended to teach lessons, but to remind staff of the threats to security and of the principal security measures necessary to combat them. To retain their impact, posters must not only be prominently displayed but also frequently changed.

6. Wall Calendars. These, featuring a different security theme for each month, particularly when well designed, can be very effective in pressing home the security message.

7. **Stickers**. Stickers are aimed at reminding staff of their personal responsibility for maintaining security, when using specific items of security equipment (eg the

secure use of the telephone and of computers). Stickers should be placed on, or adjacent to, the equipment concerned, but not on security containers.

8. **Security Service posters and stickers** are advertised through a catalogue called "Security Education Material" (97-98) etc. It is published annually and is given publicity in Security Education News - see para 1328. The posters/stickers may then be demanded from CSE Llangennech.

9. **Security aide-memoires**. Security aide-memoires should be produced at unprotected level, though, on occasions, they may need to be protectively marked RESTRICTED. These will be of particular value for newly inducted staff.

Note: Many security training aids produced by other Agencies, such as those advertised in "Security Education Material" and "Security Education News", now attract a cost.

ANNEX C

SECURITY TRAINING: INSTRUCTIONAL METHODS

1. The choice of method will depend on the specific training requirements (which must first be clearly identified), on the nature of the target audience and on the degree to which it is desirable that those in the audience should participate in the course. However, whatever medium of instruction is adopted, there should always be an opportunity for some participation by the audience, if only in provision for questions.

2. As a general guide, if only one subject is to be covered, a talk may be the most appropriate medium. It is useful to confirm the audience's understanding of the talk with subsequent discussion. It is also important to consider the size and composition of the audience. For example, it may be difficult to pitch a talk to capture and retain the interest of groups comprising widely different seniorities or specialisations. Large audiences may pose problems - audibility, reduced impact of the message on the individual, and the tendency for individuals to feel anonymous in a crowd and therefore to listen and contribute less.

3. **Seminars or informal talks**. Seminars or informal talks may be useful when a greater degree of audience participation and discussion is possible and desirable, for example:

   a. When persuading senior management of the importance of promoting good security practice; or

   b. When introducing staff to the security requirements of a specific task.

4. If a wider variety of topics of general needs to be covered, a presentation with different speakers may best hold the attention of the group, and help them to distinguish between the different subjects.

5. When a greater amount of information is to be conveyed, and the students need to understand and apply it, a longer course may be desirable, with opportunities for practical exercises to ensure that the audience understands and retains the information.

6. With both presentations and courses, frequent question and answer periods provide a change of pace and the opportunity of digesting the information. Such periods need to be guided or simulated by the course staff.

7. Appropriate visual aids (eg multimedia, the overhead projector, slides and the display board) should, whenever possible, be used to reinforce the effect of the

spoken word. Clear and simple aids that enhance the talk but do not distract the audience should be used.

ANNEX D

SECURITY TRAINING: MULTIMEDIA LEARNING

Introduction

1. Essentially, multimedia involves the use of text, graphic and animation files, photographic images and sound and video clips to create dynamic, computer based information delivery and learning products. Multimedia products are invariably packaged, ie recorded in a simplified playable format, on CD ROMs (Compact Disk Read Only Memory). Each CD can store up to the equivalent of 650 million characters and can be played on a compatible multimedia system.

2. The basic stand alone multimedia system differs from the standard personal computer, or laptop, in that it includes a CD ROM drive, sound card and separate speakers. Some systems include a MPEG (Motion Picture Expert Group) card that allows full screen viewing of video clips without loss of picture quality.

Multimedia Products

3. A comprehensive array of commercial multimedia products is available to support a wide range of activities, all of which are essential to the workings of any organisation. These include:

a. Training/education.

b. Information Management.

c. Product catalogues.

d. Advertising.

e. Presentations.

Multimedia Advantages

4. The quality of multimedia products available is evidence of a growing reliance on the use of these types of media: they provide cheap, though highly effective methods of delivering information, education and training. Take training as an example: on the one hand, over the past few years many organisations have

slashed their training budgets and reduced their training resources. On the other, the need for training has risen relative to the

rapid changes in technologies and working practices in the workplace. Consequently, organisations have been forced to reassess how they provide appropriate training for their employees.

Computer Based Learning (CBL)

5. Many organisations have found that CBL provide a viable alternative to increasingly expensive traditional classroom-based/trainer-led teaching methods. The CBL approach is being adopted by many organisations as the main impetus to their training strategy. Reduced training budgets and a corresponding decrease in cost, increase in capability and enhanced user friendliness of modern IT systems; and the development of CD ROM multimedia products serve to make the use of CBL products all the more attractive.

Benefits of CBL

6. Organisations using CBL as part of the whole of their training strategy have reported the following benefits when comparing CBL with traditional teaching methods; that it:-

a. Provides effective training, because it:

(1) gets training to the point of need, irrespective of geographical location;

(2) can be used for revision or for reference material;

(3) can cover subjects from learning to type to servicing complex aero engines.

b. Speeds up learning and project implementation, because:

(1) the dynamics of multimedia products promote learning;

(2) 100s or 1000s of employees can be trained simultaneously;

(3) CBL is 30% more effective than traditional forms of training.

c. Takes much of the stress out of learning, because:

(1) individuals work at their own speed;

(2) there is no peer pressure;

(3) self evaluation occurs;

(4) there is no travelling or staying away from home;

(5) it is fun to use, so individuals learn and retain more.

d. Saves money, by:

(1) making better use of resources;

(2) being cheaper to produce and distribute;

(3) being easy to update;

(4) saving high costs of travel and subsistence;

(5) saving staff time to and from training centres;

(6) requiring no, or reduced training, resources.

The Way Forward

7. To make the best use of resources the Security Service has set up a multimedia production group. The group comprises qualified trainers with multimedia authorising skills. They are responsible for identifying, analysing and developing appropriate multimedia products in support of our protective security advisory and education roles. As a pilot scheme the Security Service has produced a CBL package which deals with the handling of sensitive intelligence. This package has been distributed for use by thousands of individuals dispersed worldwide. Its cost works out at about 42.5 pence per user!

This page intentionally left blank.

CHAPTER 14

SECURITY ON OPERATIONS – SECURITY ELEMENTS OF FORCE PROTECTION

This page intentionally left blank

CHAPTER 14

SECURITY ON OPERATIONS – SECURITY ELEMENTS OF FORCE PROTECTION

General

1401. JSP 440 has been written with the aim of setting out the principles of security and providing the guidelines and instructions required to maintain security throughout the Ministry of Defence.

1402. Surprise and security are two of the principles of war; surprise cannot be achieved without good security. On operations, the tempo, nature and extent of activity may preclude carrying out in full the detailed security procedures outlined elsewhere in JSP 440. This is not to suggest that security on operations is of less importance than at peacetime base locations or on exercises. Indeed, the success of operations depends in great measure on the element of surprise and on the steps taken to prevent knowledge of friendly force intentions reaching the adversary; security enhances freedom of action by limiting vulnerability to adversary activities and threats. Thus, security on operations is based primarily on the security of information. The main object is to prevent the adversary obtaining information about our intentions, order of battle, vulnerabilities, deployment and movements. In certain types of operations, especially where terrorism is involved, measures required to prevent the seizure of arms, ammunition and equipment, and attacks against our own forces with, for example, improvised explosive devices, also assume significant importance.

1403. Although the detailed procedures given elsewhere in JSP 440 may not all be fully appropriate to the operational scenario, the principles upon which these procedures are based remain equally valid in both peace and war.

1404. The aim of this chapter is to provide general guidance to assist commanders to produce their own security orders while deployed on operations ranging from minor conflict to general war. To ensure that all personnel are familiar with their responsibilities, these procedures are to be practised on exercises as appropriate.

1405. A clear distinction must be drawn between security on operations and operations security (OPSEC). OPSEC is "the process which gives a military operation or exercise appropriate security, using passive or active means, to deny the adversary knowledge of the dispositions, capabilities and intentions of friendly forces" (AAP-6(U)). The OPSEC plan provides for the **overall** security of an exercise or operation, employing a wide range of military disciplines: both offensively, to disrupt or destroy the adversary's intelligence, surveillance, target acquisition and reconnaissance (ISTAR) capability; and defensively, to deny information to the adversary. The OPSEC plan will, of course, include measures and procedures taken as part of security

on operations. Further information and details of OPSEC can be found in AJP-01 and JDP 3/98.

Force Protection

1406. In future conflict, the emphasis will be on joint operations with UK forces operating as part of a multinational force. The battlespace will be non-linear with few or no 'safe' areas, and the Host Nation administration may well have collapsed, exposing the force to a wide range of threats. Security and protection, as key components of capability, assume an even higher importance in joint operations. JDP 1/99 considers UK doctrine for Force Protection in a joint and multinational context and provides a framework for comprehensive protection of the deployed force to conserve its fighting strength, in order to achieve its mission with minimum casualties to both personnel and equipment. The UK doctrine examines, within the context of joint operations, future conflict and the need for Force Protection, its aim, definitions and principles; its constituent elements; a concept of operations; and its command and control. The protection of the force, including the force generation phase, on the UK mainland, in NI and permanent garrisons abroad is addressed by existing MOD and theatre policy covering standing security measures although such policy may be modified in response to other operations.

1407. Force Protection can be defined as ***a process which aims to conserve the fighting potential of the deployed force by countering the wider threat to all its elements from adversary, natural and human hazards, and fratricide***. Force Protection is not an issue that can be addressed separately or in isolation. It is an integral part of operations and must be incorporated into the Commander's plan from the outset. In Joint Operations involving UK forces overseas the CJO's Strategic Estimate will consider Force Protection as a factor, and this should be reflected in the deployed force levels. The Force HQ will examine Force Protection in more detail in the Operational Estimate, which will confirm Force Protection policy and security requirements based on the threat assessment.

Security Elements of Force Protection Measures

1408. Following the threat assessment, appropriate protective measures can be decided. Force Protection measures fall under several broad categories which includes security covering physical and procedural measures, directed from Force HQ level and integrated into the overall plan, but mainly applied at local level. Security measures aim to minimize direct and indirect attacks on personnel, equipment, installations and lines of communication by other than the adversary's main forces. In OOTW and PSO, where the adversary may not possess an air, theatre missile and NBC capability, security is probably the main constituent of Force Protection. Some security measures will affect the civil population, and such measures must be subject to appropriate legal advice which may need to incorporate the requirements of international law, Host Nation law, and any extant status of

forces agreements or Memoranda of Understanding (MoU). Security measures incorporate:

a. **Personal Security**. Standing physical and procedural measures to protect personnel.

b. **Physical Security**. Physical and procedural measures to protect positions, installations and units from attack, sabotage and theft.

c. **Lines of Communication Defence.** Patrols, mine clearance, overwatch, bridge guards, etc, to ensure the safety and security of lines of communication.

d. **Security of Information**. Physical and procedural barriers to protect friendly information. The deliberate or inadvertent compromise of protectively marked information by the Media is a risk, and this aspect should be specifically addressed by Force HQ and unit instructions. Levels of access afforded to the media, and the ability to control this, will also have an impact on Force Protection.

e. **Liaison with Host Nation Security Forces.** Where the host nation security forces retain some operational capability, liaison is vital to co-ordinate actions. In some cases Host Nation security forces may have primacy, in nearly all they can provide intelligence and other related information about conditions in theatre.

f. **Civil Population Control.** Refugee and displaced persons, border and port controls, curfews and other restrictions, to minimize civil population interference with operations.

g. **Prisoners of War (PW) and Detainees.** Secure accommodation and guard forces will be required to contain PW and detainees.

Responsibility for Security

1409. Security remains a command responsibility on operations. On operations, where a commander considers that the full procedures detailed elsewhere in JSP 440 are impossible to carry out without adversely affecting the conduct of the operation and achievement of the mission. It is the responsibility of the commander to modify the existing security procedures applicable to the force in accordance with the established principles described in JSP 440. Such modifications are to be agreed by at least a one-star commander. The modifications ordered by a commander in the field are to be notified to PJHQ through the normal security chain and Force HQ.

1410. A suggested outline of staff responsibilities for security in a Force HQ on operations is at Annex A.

Security Orders

1411. Requirement. Force HQ security staff are responsible for the preparation and issue of security orders for operations and deployments. A checklist of headings that should be used in security orders is at Annex B. Not all headings need be used but security plans should include countering specific threats and must be reviewed regularly to adjust to changes in the threat. Security orders must provide for the denial to the adversary of information and intelligence received directly or indirectly from for example:

a. Imagery intelligence (IMINT) from both aerial reconnaissance flights and satellite platforms.

b. Signals intelligence (SIGINT) covering information obtained from the interception of communications (COMINT), including direction finding, and non-communications emissions (ELINT), e.g: radar.

c. Human intelligence (HUMINT) including manned reconnaissance, patrol reports, interrogation of prisoners of war (PW), espionage and loose talk.

d. Loss or compromise of sensitive and protectively marked documents, including soft copy.

e. The physical protection of personnel from terrorist attack (e.g: assassination).

f. The protection of personnel from seditious or subversive influences likely to undermine morale, e.g: propaganda and rumours.

g. The safeguarding of protectively marked and vital assets from sabotage or capture by adversary special forces or local sympathizers.

Principles

1412. The following principles must be observed.

a. The commander at every level is responsible for security within his command.

b. Security should enhance an operation; not constrain it.

c. Security planning must start at the highest level with the initial concept of operations and be integral to operational planning.

d. All personnel must be made continually aware of the threat to security, how it affects them individually and their specific responsibilities for countering it. A security briefing checklist is at Annex C.

e. Every individual who handles protectively marked information and protectively marked or vital materiel is personally responsible for safeguarding it in the appropriate manner.

f. Protectively marked information may normally only be given to those who have been cleared to the appropriate level of security clearance and who need the information to carry out their duties.

Threat Assessment

1413. Responsibility. Force Protection is a risk management process based on the threat assessment, the results of which determine measures addressing: overall and collective protection; security; and health and safety. Over-protection to counter an improbable threat can divert scarce resources from achieving the mission. An overall threat assessment (which should include the protagonists' current and possible future intent derived from their aims, doctrine, culture and history) will be conducted at MOD/PJHQ level as part of the planning process. An overall assessment of Force Protection requirements based on this threat assessment should be incorporated into the CDS directive. Once the force has deployed, the Force HQ will refine this threat assessment as part of the Joint Task Force Commander's (JTFC) estimate and directive. Additional localized assessments will need to be conducted, particularly in OOTW and Peace Support Operations (PSO), where the threat may vary. Where more than one adversary exists, their intents, threats and capabilities must be included in the threat assessment. This may reveal a threat to the UK mainland or UK forces in other theatres arising from a conflict, which may include non-violent activities such as PSYOPS and other associated tactics aimed at influencing international perceptions. Countering such threats will be the responsibility of the local authorities. The threat assessment should consider the following security elements:

a. The adversary's military intelligence, surveillance, target acquisition and reconnaissance (ISTAR) assets and capabilities - can he detect and locate friendly activities?

b. The adversary's espionage and covert intelligence capability. Does he have operatives in the Joint Operations Area (JOA)?

c. The adversary's capability to conduct Information Operations (INFO OPS) and Command and Control Warfare (C2W) activities, including those aimed at audiences and targets outside the JOA.

d. The adversary's EW (including Directed Energy (DE) weapons) capability. Can he intercept, direction find, jam or interfere with friendly transmissions?

e. Adversary sympathizers, agents and partisans in the JOA. Will they conduct information gathering, espionage or guerrilla acts against us?

f. Terrorist, criminal and insurgent organisations. What are their aims, capabilities and methods? Do they, for example, include hostage taking as a tactic?

g. The attitude of the civil population and refugees or displaced persons (by region, if appropriate) to the military presence. Are they hostile, neutral or favourably disposed towards us? Could their perceptions be altered by friendly or adversary actions, including INFO OPS?

h. Sabotage, in the form of planned attacks by adversary special forces or other agents, or more spontaneous activities by locally employed civilians.

i. Subversion and Hostile PSYOPS. It is likely that an adversary will attempt to subvert friendly forces, either individually, to gain leverage, or collectively for political and military advantage.

Likely Tasks of Adversary Intelligence

1414. Adversary intelligence requirements are likely to include the collection of information on the following aspects of friendly force activity:

a. Future intentions.

b. Operational plans and capabilities, including those of reservists.

c. Communications, command and control.

d. Protectively marked equipment.

e. Order of battle.

f. Strength and morale of forces.

g. Intelligence organization, particularly the extent of our knowledge of the adversary and how information is gathered.

h. Logistics including details of resources, reinforcement plans and equipment replacement.

i. Casualties in men and materiel. Results of adversary action.

j. Security organization and our knowledge of the adversary's espionage, sabotage and subversive activities.

k. Personnel vulnerabilities, e.g: character weaknesses, etc, of individuals which could be used to coerce them into working for the adversary. (This would normally be expected to pertain during protracted operations).

l. Identification of key personnel and their future movement plans.

Protection of Potential Targets

1415. Security of information. The principal sources from which the adversary will attempt to derive information are:

a. **Surveillance and reconnaissance.** Every unit and HQ must take appropriate action to deny the adversary direct observation from ground and air. This includes use of sanitized areas surrounding C^3 facilities, camouflage and concealment, track discipline, night movement and use of cover.

b. **Radio and line communications.** All messages sent by radio are liable to interception by the adversary. Similarly, although to a lesser degree, messages sent by landline can also be intercepted by the adversary. The importance of the strict application of communications security procedures laid down in Chapter 9 is particularly important.

c. **Non-communications emissions.** Emissions from across the electromagnetic spectrum (TEMPEST) are all liable to detection and interception by the adversary. Security orders are to include the defensive measures necessary to defeat the adversary's efforts in this area. Particular attention should be paid to:

(1) Electronic emissions, e.g: radar and radiation from IT systems.

(2) Thermal emissions, e.g: from vehicle engines and exhausts.

d. **Documents and information technology (IT) systems.** Documents, which include such items as maps and computer discs are particularly valuable sources of information. All documents whether private or official, must be considered to contain matters of interest to the adversary. Detailed guidance on the security of documents is given at Annex D. The primary risk to IT systems is loss of data either by capture or physical loss or damage. IT Systems which are intended for deployment on operations are to have appropriate countermeasures detailed in the System Security Policy (SSP) and the Security Operating Procedures (SyOPs).

e. **Loose talk.** Any conversation may be overhead and ultimately communicated to the adversary.

f. **Discussions and briefings.** Discussions and briefings within HQs and units on the subjects in paragraph 1414 above should as far as possible take place only in areas where positive access control is in place and formal counter eavesdropping measures have been taken.

g. **Private correspondence.** All private correspondence in transit to and from units should be handled by the Defence Postal and Courier Service. When appropriate, and on the orders of the force commander, private correspondence will be subject to censorship. Guidance is at Annex E.

h. **Private telephone calls.** Similar restrictions to those applying to written correspondence apply to private telephone conversations. Annex E applies. On occasions when commanders consider it operationally necessary, private telephone calls may be prohibited.

i. **The media.** When circumstances warrant it, a system to control the movement and output of accredited correspondents will be authorized. Instructions for the implementation of this system, designed to ensure that aspects of our operations and plans are not jeopardized in any way, will be issued by the Ministry of Defence.

j. **Civilians.** Civilians who remain in the area of operations may deliberately or by accident come into possession of information of value to the adversary. Effective measures should be taken to control their movement so that they cannot become a source of leakage. In particular, civilians with legitimate access to an operational area, e.g: traders and workmen, are to be prevented from having access to protectively marked information and, if this is not possible, should be appropriately security cleared.

k. **Destruction.** Emergency destruction methods must be prepared for immediate use from the outset of operations. See Chapter 5 for information on methods of destruction.

l. **Prisoners of war.** Every officer and soldier must understand their individual responsibilities in the event of capture.

1416. Security of personnel. The adversary may attempt to undermine the morale of our own troops and to breed disaffection using the following main methods:

a. **Propaganda.** Propaganda may be spread by adversary radio and television stations or by leaflets distributed from the air, by shell or by agents. The best counter is the briefing of all personnel in the methods and aims of adversary propaganda and the dangers of naive acceptance.

b. **Subversion.** Any identification of subversive activity is to be reported immediately to the Force HQ security staff.

c. **Rumours.** All personnel must be instructed to check rumours and speculation and to report instances immediately to the unit security officer. Authoritative statements by Force HQ can quell rumours at an early stage.

1417. Security of materiel. The key factors in countering sabotage of all types, including minor damage and pilferage of materiel, are a well trained and supervised guard force, strict physical security controls, and effective access control.

1418. Personal security. The adversary will attempt to assassinate or capture key personnel. Likely adversary targets should be identified by the Force HQ security staff in consultation with the intelligence branch. Trained close protection (CP) teams should be deployed by the appropriate staff to protect these individuals. Details of the movement plans of such individuals should be kept on a strict need-to-know basis.

Procedures

1419. Security of operations. Security must be an integral part of all operational plans. To be effective security must be considered from the earliest stages of operational planning. Steps to be considered are:

a. Strict adherence to the "need-to-know" principle for all plans, but ensuring that information is distributed widely enough to enable all those involved to carry out their role effectively.

b. Responsibility for interpreting the "need-to-know" of troops on operations rests with the commander concerned. This includes the issuing of short term protectively marked battle information to all those who need to know it for operational reasons, regardless of their security clearance.

c. Keeping the number of copies of plans and associated documents to a minimum - the "need-to-know" principle.

d. Good communications security.

1420. Physical security. Detailed physical security arrangements for HQs and units in the field will depend on the local threat and on the type of HQ or unit concerned. The following points are to be considered:

a. Control of access.

b. Use of a 'sanitized area'.

c. Track discipline.

d. Camouflage and concealment.

e. Vehicle parking.

f. Noise control.

g. Lighting control.

h. Security of arms, ammunition and explosives.

i. Security of documents. See Annex D.

j. Security of materiel - Both protectively marked and unclassified.

k. Procedures for codewords, nicknames and passwords. See Annex F.

l. Constant review of SOPs - based on experience, fresh reports and recurring problem areas.

Rôle of Security Units on Operations

1421. Specialist security tasks in the field are carried out by specialist security units as directed by the Force HQ security staff. The priority allocated to and necessity for these tasks which are listed below will vary according to the intensity of the conflict and the different stages of friendly operations, e.g: offensive, defensive or consolidation phases.

a. **Protective Security Tasks**.

(1) To issue orders on, or provide advice on protective security measures to be taken by HQs and units.

(2) To issue or provide advice on orders for static guard forces as appropriate.

(3) To advise on the security aspects of arrangements for the protection of key points.

(4) To carry out rapid investigations into breaches of security.

(5) To advise on methods for the emergency destruction of protectively marked documents and materiel likely to be of use to the adversary.

(6) To advise the OPSEC staff on, and in conjunction with that staff, monitor the implementation of relevant OPSEC measures.

(7) Security checks and vetting of locally employed labour.

(8) In order to deny information to the adversary, friendly force security personnel are to carry out security sweeps of evacuated HQs and unit areas to ensure that security measures, e.g: the destruction or removal of documents have been carried out.

(9) Abandoned equipment and vehicles, including aircraft, are also to be searched, preferably by unit personnel familiar with the item, to

ensure they contain no information of use to the adversary and destroyed.

(10) Security personnel are to be among the last to leave an area or installation, in order to carry out security sweeps.

(11) When the operational situation demands and within legal constraints, to search civic and public offices, police stations, banks, etc, as appropriate for civil records and to arrange for the safe custody of such documents that are vital for subsequent civil administration or the investigation of war crimes, or may be of value to the adversary.

(12) To provide advice and assistance to units in the implementation of censorship if ordered and to raise base censorship units if authorized.

(13) To ensure that captured adversary materiel of intelligence interest is put in safe custody prior to exploitation.

(14) To ensure that until such time as they are taken over by communications staff or units, no radio, television or telephone installations are available for use by adversary sympathizers.

(15) To maintain security records.

b. **Security Intelligence Tasks.**

(1) To search captured adversary HQs and static locations, including living quarters of senior officers, for materiel of intelligence and security interest. Security personnel must be available to enter previously held adversary areas and HQs immediately after these have been captured. It is essential to try to prevent destruction of materiel by the adversary. Friendly forces need to be briefed in advance not to destroy or incapacitate in any way captured adversary materiel or documents. Procedures for passing items of immediate tactical value to the intelligence staff are to be in place.

(2) Liaison, if appropriate, with Host Nation intelligence, security and police forces.

(3) To collect security intelligence on the identity, capabilities and intentions of adversary intelligence services, their agents and informers, in order to take action to counter their plans.

(4) To identify and prevent espionage and sabotage activities by adversary agents and sympathizers.

(5) To carry out the rapid investigation of any incidents suspected of being caused by adversary sympathizers or agents.

(6) To carry out the questioning of suspects for information of security value. This task will often include, in addition, questioning for tactical information.

(7) To make contact with friendly agents and known sympathizers who may have useful information about the adversary which is of tactical importance.

(8) To make contacts with civil authorities and reliable civilians who may form the basis of an information service.

(9) To round up known adversary agents, sympathizers or suspects.

(10) To advise on the state of civil administration, its operation and reliability where it affects friendly operations.

(11) To maintain, in conjunction with the Service police and if appropriate, Host Nation police, security controls over the civil population, especially refugees. As far as possible refugees should be canalized and checked at control posts to guard against infiltration by adversary agents. Children may be used by the adversary as messengers and must also be checked.

(12) To advise on and to take action to prevent civil disturbance or subversive activity from interfering with operations.

(13) To supervise and check the application of civil controls, e.g: curfews, restrictions on movement and communications, registration and issue of identity cards to civilians.

(14) To provide advice and assistance on the security aspects of travel through seaports, airports and across land frontiers, and to act as travel control security units if authorized. Details of the functioning of a travel control security unit are at Annex G.

(15) To assist in maintaining morale by checking rumours and attempts by adversary sympathizers to spread adversary propaganda.

(16) To maintain security intelligence records.

ANNEX A TO CHAPTER 14

SUGGESTED OUTLINE OF STAFF RESPONSIBILITIES FOR SECURITY WITHIN A FORCE HQ ON OPERATIONS

Chief J2

Advice to the force commander on all aspects of Force security.

Implementation of Force security policy.

Direction of the work of the Force HQ security staff.

Direction and tasking of Force security units.

Dissemination policy for protectively marked information.

Production and dissemination of threat assessments.

SO2/SO3 J2(X)

Organization and day to day direction of the Force HQ security staff.

Implementation of aspects of security policy as directed.

Security of operations and plans.

Staff work concerned with security investigations carried out by security units

Direction of all protective security measures including the arrangements for the handling and custody of protectively marked documents, and vetting or screening of locally employed personnel, within Force HQ.

Planning and implementation of measures for travel control security.

Force HQ security officer and vetting records officer.

Issue of security standing orders, instructions and operating procedures.

Direction of security checks and inspections.

Liaison with Media Ops Staff on release of information.

SO2/SO3 J2(SP)

Control of access to and dissemination of information from special communications cell.

Branch Security Officers (BSOs)

Supervision of all security arrangements and implementation of security orders within their branch.

Production of branch security orders.

Initial investigation of all security incidents within their branch and subsequent requests (if appropriate) for security unit involvement.

Checks and inspections of branch security arrangements.

Control of access to their branch.

Ensuring that all branch personnel are fully aware of security procedures.

ANNEX B TO CHAPTER 14

CHECK LIST OF SECURITY ASPECTS TO BE COVERED IN SECURITY ORDERS

The following security matters need to be addressed as soon as an operation is envisaged.

(The list is not exhaustive, nor will items apply under all circumstances.)

1. Appointment of a security officer reporting directly to the force commander.

2. Allotment of tasks to security personnel.

3. Provision of threat assessments.

4. Notification of codewords and nicknames with meanings.

5. Timings of release of information into the public domain.

6. Security areas and system of access control.

7. Identifying requirements for guarding personnel, material and locations.

8. Custody and storage of protectively marked documents.

9. Security clearances of Service personnel.

10. Security clearances and control of visitors.

11. Protection from overlooking and eavesdropping.

12. Protection and storage of protectively marked materiel, equipment, arms, ammunition and explosives.

13. Delivery and dispatch of protectively marked documents and materiel.

14. Clearance of security areas.

15. Destruction of protectively marked documents, materiel and waste (including emergency destruction plans).

16. Dangers of hostile intelligence service radio and electronic interception.

17. Communication electronic security precautions, including cover and deception plans.

18. Restrictions on radar and radio testing and the use of radio communications.

19. Protective EW arrangements.

20. Physical security of protectively marked communications equipment.

21. Telephone security.

22. Action on capture of adversary arms, ammunition and explosives.

23. Action on capture of adversary documents and materiel.

ANNEX C TO CHAPTER 14

SECURITY BRIEFING FOR PERSONNEL DEPLOYING ON OPERATIONS

Briefing

1. All personnel deploying on operations are to be briefed on the following subjects where applicable:

a. The threat. This should cover all phases of the operation and all areas involved, e.g: ports of entry and exit, staging ports and in theatre.

b. Security of arms, ammunition and explosives.

c. Security of sensitive and protectively marked documents.

d. Security of information and IT systems.

e. The security risks inherent in conversation with civilians prior to, during and after operations. The need to report any suspicious approach which may be made by civilians.

f. The need to be alert and to report suspicious activity.

g. Communications security.

h. The security of protectively marked materiel and equipment.

i. Security measures required to counter hostile surveillance. Such instruction may form part of SOPs or unit security standing orders. (This area is primarily an OPSEC matter but should be included where relevant).

j. The action to be taken by personnel when the presence of any civilian is noticed who appears to be taking undue interest in the preparations, or taking hostile action during the operation, e.g: loitering near a unit or HQ or taking photographs, making notes, or interfering with military property such as communication cables.

Security of Arms and Ammunition

2. Commanders are to issue written orders on the safeguarding of arms, ammunition and explosives. These orders are to be framed with particular attention to the following:

a. Establishment of armouries or properly guarded stores where applicable.

b. Control and recording the issue and receipt of arms, ammunition and explosives.

c. The responsibility of individuals for the security of arms, ammunition and explosives issued to them and the procedures for handover.

d. Highlighting the recovery phase of the operation as being a period requiring especially tight control.

e. A tally is to be made of all arms, ammunition and explosives on personal issue. These items are also to be checked before and after moves to other locations. (On return to unit, arms, ammunition and explosives are to be checked (arms by registered number) and immediately stored in a secure armoury or magazine).

f. Implementation of Force HQ policy concerning the handing-in of captured weapons or "souvenirs".

Security of Protectively Marked Documents

3. There is a particular need to safeguard protectively marked documents and materiel during operations especially those held in vehicles. SOPs are to include arrangements to control access to vehicles containing protectively marked materiel including aggregations of RESTRICTED information which may merit a higher protective marking.

4. Only those protectively marked documents that are essential for use during an operation are to be removed from their normal secure place of storage and taken into the field. Such documents are to be protected as follows:

a. Prior to deploying they are to be listed and booked out on signature to the appointed unit security officer. At this stage they are to be checked for completeness by page identification and page counting.

b. The individual who is normally responsible for their accounting and safe custody is to retain a copy of the list. Should the unit security officer issue the documents further, he is to do so on signature to those individuals who need to use them. If the documents are destroyed this should be supported by an appropriate witness signature.

c. They are to be stored in document security boxes or such other containers of approved security pattern when not in use. These boxes are, where possible, to be firmly affixed to the framework of vehicles. Vehicles and containers containing protectively marked documents are never to be left

unattended when not in use. The normal rules for controlling access to protectively marked documents are to be applied at all times.

d. At the end of the operation the branch or unit security officer is to recall all documents issued by him and check them for completeness. On completion of the recovery phase he is to return them to the owning individual where they are to be checked once more for completeness, as in sub-paragraph a above, before being returned to their normal place of storage.

5. Protectively marked documents originated or received on operations are to be accounted for (and protected as far as is possible) in accordance with the instructions given by the force commander. Exceptionally, however, the instructions below in respect of Protected Document Registers (MOD Forms 102) are to be followed:

a. Current registers are not to be taken on operations. A separate register is to be taken into use and an officer or nominated clerk is to be appointed to maintain it. An officer is to be nominated, on the first page of the register, to supervise its maintenance.

b. All documents protectively marked SECRET and above originated, received and dispatched during the operation are to be recorded in the register. In the event that TOP SECRET documents are handled, a TOP SECRET Control Officer is to be appointed to maintain a register in which TOP SECRET documents are to be accounted for.

c. At the end of the operation the details of those protectively marked documents that are still required to be held are to be transferred to a current register and the documents filed and stored in accordance with normal rules. All other protectively marked documents are to be destroyed in accordance with the instructions for their protective marking.

d. When all details in the register have been deleted the register is to be closed formally and retained for one year.

6. A l00 per cent check of those essential policy and reference documents protectively marked TOP SECRET is to be carried out daily. TOP SECRET documents that are dependent on the operational situation for their degree of protective marking are to be subject to checks as laid down by the force commander. A l00 per cent check of all extant TOP SECRET documents is to be carried out at the end of the operation.

7. Before vacating any location an inspection is to be made to ensure that no protectively marked materiel or other sensitive documents have been left in the area. Where possible an inspection is also to be made at first light the following morning whenever a site is vacated during the hours of darkness.

8. Protectively marked documents may, where practicable, be destroyed in the field. If shredding is impracticable, protectively marked waste is to be collected daily, and destroyed by burning. The rules for recording the destruction of documents, protectively marked SECRET or above, are to be observed.

Security of Protectively Marked Equipment

9. Commanders of units with equipment protectively marked CONFIDENTIAL or above are to issue written instructions for its security protection.

10. Such instructions may form part of SOPs or Security Standing Orders. They are to include:

a. The need for physical checks of the equipment during all phases of the operation and at each location as appropriate (including whilst under repair).

b. Control of access to the equipment at all times.

c. Action to be taken to safeguard the equipment in the event of breakdown, traffic accident, or recovery of the equipment to a repair facility.

d. The protection to be afforded the equipment against the activities of adversary and hostile intelligence units, their agents and informers, and other unauthorized persons. In particular, instructions are to specify the precautions to be taken against:

(1) **Surveillance.** Where appropriate measures are to provide protection against sophisticated surveillance devices (e.g: optical, acoustic, seismic, magnetic, radar, image intensification and thermal imaging) as well as against simple visual observation by a ground or air observer. Defences against sophisticated devices need to be based on specialist advice available through Force HQ security staff.

(2) **Intercept.** Where appropriate measures are to provide protection against the interception of non-communications electronic emissions, e.g: radar in weapons systems (see paragraph 1415).

Operations News Sheets

11. If news sheets are issued during an operation they are not to contain any protectively marked information. Care is to be taken in reporting the progress of the operation not to disclose any orders of battle, aims of the operation, special battle techniques, special weapons or any other matters that may not be made public.

Security of Protectively Marked Documents and Equipment when in Contact with the Adversary

12. When it is essential for operational reasons for protectively marked documents or equipment to be taken into situations where a part or the whole of the operational plan involves direct conflict with the adversary, a list of equipment being taken is to be notified to the next higher formation and copies of all protectively marked documents taken are also to be held by them; so that in the event of capture or compromise swift damage assessments can be made and timely counter-measures taken.

13. Those in charge of or carrying protectively marked documents and equipment must be aware of the priority for destruction of protectively marked items in the event of imminent capture.

This page intentionally left blank

ANNEX D TO

CHAPTER 14

SECURITY OF DOCUMENTS ON OPERATIONS

General

1. The protection of documents in the field from unauthorized access, disclosure or loss is dependent on the proper application of:

a. Clear and detailed security orders.

b. Protective markings.

c. The "need-to-know" principle.

d. Physical security measures.

2. On operations, as in peacetime, it is necessary for every establishment holding documents protectively marked SECRET or above to know what documents it holds and where they are. In order to do this a record must be kept. The aim is to record, in the simplest form possible, the minimum information required, consistent with operational circumstances and the local threat.

Protectively Marked Documents

3. **Dispensations from peacetime procedures for the handling of protectively marked documents.** On operations in the field, a commander may consider that the full procedures detailed elsewhere in JSP 440 are impossible to carry out without adversely affecting the conduct of the operation or achievement of the mission. It is the responsibility of the commander to modify existing security procedures for protectively marked documents as necessary in accordance with the established principles described elsewhere in JSP 440. In these circumstances the modifications ordered by the commander in the field are to be agreed by a one-star commander and notified through the normal security chain to the Force HQ security staff.

Registration of Documents

4. Prior to deciding that the use of the Protected Document Register (MOD Form 102) for protectively marked documents marked SECRET and above is not possible without adversely affecting operations, a commander should consider whether the continued use of the register for TOP SECRET and CODEWORD material should

continue. If not, he should consider the possibility of each unit keeping a record in the appropriate log. The following details should be entered in the log:

a. The communications head serial number (which is marked in the top right corner of every message received or transmitted by the communications centre of formation HQ), or other short reference in the case of messages delivered by other means, e.g: by liaison officer.

b. The reference number of the battle board clip or file into which the message is filed by the unit.

c. A unique folio, enclosure or sheet number.

5. In the event of a commander deciding that operational circumstances are such that it is necessary to suspend the majority or even all protectively marked document record keeping, he should consider basing the security protection of documents marked SECRET or above on the establishment of controlled areas:

a. Within which no protectively marked document records need be maintained.

b. To and from which access is strictly controlled at all times.

c. From which no document marked SECRET or above is removed except for despatch or destruction.

Checks

6. Checks of documents marked SECRET and above, should be made at appropriate intervals laid down by the Force HQ security staff.

Destruction

7. All protectively marked documents taken into the field are to be reviewed for destruction on a daily basis.

8. In certain operational circumstances a commander may decide that destruction in accordance with normal procedures is not possible without adversely affecting operations. In this event he should order destruction by the most secure means available.

9. Protectively marked documents must not be allowed to fall into adversary hands. For example, in the event of adversary penetration threatening to overrun a position and capture protectively marked documents, the documents are to be destroyed or otherwise denied to the adversary by whatever means are available.

Safeguards During Moves

10. Protectively marked documents are to be securely packed in secure containers approved by the Force HQ security staff. Such containers are to be safeguarded at all times.

Safeguards on Operations

11. Protectively marked documents that are not in use but are still required to be held are to be stored in locked secure containers approved by the Force HQ.

12. Approved containers containing protectively marked documents are not to be left unattended. Where appropriate, containers should be securely anchored, e.g: bolted to an appropriate structure, to prevent them being easily removed.

13. Keys to approved containers are to be safeguarded.

14. Displays of protectively marked information are to be mounted in such a way that they cannot be seen by anyone who is not authorized to have access to them. Covers or curtains may be required for temporary screening from view.

15. Protectively marked documents should be held in HQs and units as far from the front line as operationally acceptable.

16. Protectively marked documents should not be carried when closing or in contact with the adversary unless operationally essential.

Loss or Compromise

17. The loss or compromise, or suspected compromise of a document marked SECRET or above is to be reported immediately to Force HQ, to the HQ or unit which originated the document, and to all other HQs and units affected. The reporting HQ or unit is to include in the report an immediate assessment of the damage caused so that counter compromise action can be taken.

Unclassified Documents

18. Unclassified documents, including letters, diaries and photographs should not be carried on operations when closing with the adversary, as they may give useful information to interrogators in the event of capture.

This page intentionally left blank

ANNEX E TO

CHAPTER 14

REGULATIONS FOR THE CONTROL OF PRIVATE CORRESPONDENCE AND TELEPHONE CALLS

1. The object of censorship can only be attained by the rigorous suppression of certain types of subject matter in correspondence.

2. Allusions to any of the following matters are forbidden at all times in private correspondence and telephone calls during operations, whether they relate to naval, military or air forces, except in specific releases authorized by the Force HQ:

a. Strength, efficiency, organization of our own or allied forces, including any comment on the absence or presence in the theatre of a unit or formation, or disclosure regarding the formation to which any unit is attached or belongs.

b. Location or movement of any naval, military or air force units or detachments, arrival or lack of reinforcements.

c. Specialist armament or equipment of any kind.

d. Distinguishing signs used for the identification of formations, units, and their transport.

e. Plans and forecasts or orders for current, future, or cancelled operations or movements, whether known or merely rumoured or surmised.

f. Communications, such as the use, condition, or probable extensions of roads, railways or other transportation facilities, bridging operations, etc.

g. State of the maintenance services, including any reference to reserves.

h. Position or description of barracks or camps.

i. Casualty figures and names of individuals before official notification and publication.

j. Effect of any action by the adversary. Any remark that may tend, if published, to encourage the adversary, to cause despondency in our own forces, people or allies, or to incite a feeling of hostility among the people in the theatre of operation or in neutral countries.

k. Criticisms and statements calculated to bring into disrepute our forces or those of our allies.

3. It is forbidden to send, or attempt to send, to unauthorized persons:

a. Official documents, including intelligence summaries, orders, reports, maps, etc, or to disclose their contents except in the course of duty.

b. Any document captured from the adversary, or found in places occupied by the adversary, and any document containing information about the adversary.

c. Any official document belonging to the civil authorities in Allied or adversary territory.

d. Objects of intelligence or research value.

e. Arms, ammunition and explosives.

4. It is forbidden to despatch to neutral or adversary countries photographs or pictorial matter of any kind, from whatever source they may have been obtained, except under conditions laid down in the censorship regulations of the Force HQ concerned.

5. It is forbidden to communicate with the press on military subjects except as laid down in theatre orders. Correspondence of a non-military nature will be permitted subject to regulations promulgated by the Force HQ.

6. It is forbidden to send through the post photographs or films except those taken under proper authority.

7. It is forbidden to invite correspondence with strangers by inserting advertisements or letters in any publication, or by any other means, or to enter into correspondence with strangers in response to such advertisements or letters. The greatest caution and reserve are necessary in acknowledging presents from unknown donors, or in replying to trade circulars from unknown merchants and dealers, especially those in neutral countries.

8. It is forbidden to make use of the civil postal service in the theatre of operations.

ANNEX F TO

CHAPTER 14

USE OF CODEWORDS, NICKNAMES AND PASSWORDS ON OPERATIONS

Definitions

1. **Codeword.** A codeword is a single word used to provide security cover for reference to a particular protectively marked matters.

2. **Nickname.** A nickname is made up of two words selected by the originator and used for convenience for reference to any matter where security protection is not required.

3. **Password.** A pre-arranged word or distinctive sound used to reply to a pre-arranged challenge.

Codewords

4. **Issue**. Codewords are issued by Force HQ to subordinate HQs on demand. Similarly, subordinate HQ are responsible for issue to units on demand. Bids for an allocation of codewords should be made as early as possible so that requirements can be met and an adequate reserve list of codewords for issue can be maintained.

5. **Recording.** A record must be kept by the issuing HQ of the following:

   a. Details of issue, cancellation and withdrawal.

   b. The protective marking of the codeword itself.

   c. The meaning of the codeword and the protective marking of the meaning of the codeword. Frequently the meaning will bear a higher protective marking than the codeword.

6. **Compromise.** If a codeword is compromised, the circumstances must be reported to the next higher HQ immediately. To minimize the risk of compromising a new codeword it must not be referred to in the same signal as the one it is replacing. When a change of codeword becomes necessary all concerned must be informed that the original has been cancelled and will be replaced by a new meaning of the codeword and should merely refer to the first signal and state:

   "Codeword is ....."..

Further guidance on codewords is given at Annex K to Chapter 4.

Nicknames

7. To prevent duplication the use of specific nicknames should be authorised by superior HQ.

Passwords

8. Force HQ is responsible for issuing a force password to be changed at 1200 hours local time daily. To avoid problems of dissemination, lists of passwords and their period of validity should be issued, sometime in advance - commensurate with the operational profile of password users.

ANNEX G TO

CHAPTER 14

TRAVEL CONTROL SECURITY (TCS)

Tasks

1. Certain operations may require the establishment of a TCS system the aim of which is to:

a. Detect and prevent entry and exit of persons suspected of being engaged in espionage, sabotage subversion or terrorism or undesirable political activity.

b. Detect and prevent the smuggling of arms, sabotage of materiel, subversive literature etc.

c. Select travellers of intelligence interest for further interrogation by the appropriate authority.

d. Provide, at appropriate levels, day to day liaison and advice on policy and operations with all concerned civilian and service departments on all aspects of TCS.

Organisation

2. Within the theatre or area concerned a TCS HQ will be formed under the command of a senior security control officer (SSCO). The duties of SSCO are outlined below. Since the work of TCS in any theatre or area will depend on the prevailing circumstances and the reliability of other control agencies they are given only in general terms.

a. To advise the commander or appropriate government authorities on the travel restrictions necessary to maintain the security of the area concerned.

b. To advise and assist in the setting up of interrogation centres for detained traveller suspects.

c. To establish and, if necessary, control the machinery for the issue of entry and exit permits.

d. To advise as to the type and method of loading and boarding passes.

e. To exercise operational control of TCS detachments.

3. The work of TCS HQ will be co-ordinated and directed by the Force HQ security staff.

4. TCS HQ will direct the work of security control officers (SCOs) who command TCS detachments at port, frontiers and airfields. The RN, Army or RAF may provide these detachments.

5. RN Liaison Officers (RNLO/RN Security Team) are allocated to Army and RAF detachments at ports, airfields, or authorized sea landing places, and at canal or river frontier crossings, of where the RN is exercising control over the waterway or airfield concerned. The duties of an RNLO/RN Area Security Team:

a. To act as liaison officer between the Army or RAF SCO and the RN authorities or the approved port authority.

b. To act as adviser to the SNA, NOIC, SNO or approved port authority in the port or area concerned on all security matters affecting TCS.

c. To ensure, in consultation with the SNA etc that all HM ships conform to the TCS regulations in force.

d. To liaise with the appropriate RN authority or approved port authority concerning such harbour, coast, river or canal patrols as may be required, and the control of vessels in harbours or prohibited coastal zones.

e. To advise, when required, on security and counter sabotage measures.

6. TCS detachments (Army) may be at frontiers, docks, ports, sea-borne landing places or in any other place as may be directed. An SCO (Army) is responsible for the examination of all persons and materiel entering or leaving the area served by the detachment. The aim is to:

a. Prevent or detect communication with the adversary.

b. Detect all agents, saboteurs or subversive persons.

c. Prevent or detect the introduction of any item that may be used for sabotage or subversive purposes.

d. Ensure that all the security control measures designed to channel all traffic through travel control posts are working smoothly.

7. TCS detachments (RAF) may be located at authorized and non-authorized airfields, landing strips, areas or in any other place as directed. The RAF Police are responsible for the examination of all persons and materiel entering or leaving the area served by the detachment. The aim is as in paragraphs 6 a - d above.

Methods

8. Control of entry into and exit from a territory is achieved by:

   a. Port control.

   b. Frontier control.

   c. Airfield control.

9. At ports, frontiers and airfields TCS falls into two broad divisions. These are:

   a. **Travel control.** This includes the examination of all persons and materiel channelled through travel control posts by a series of preventive measures known as security controls. The application of travel control principles is similar whether applied to posts, frontiers or airfields. In travel control TCS personnel have an executive function.

   b. **Security control.** This is the collective term to describe the measures designed to seal coastlines and frontiers, ports and airfields with the aim of directing all traffic through established travel control posts. The application of security control principles varies with ports, frontiers and airfields. In security control TCS personnel have an advisory function.

Travel Control

10. Travel control has two aspects common to all its posts at ports, frontiers and airfields. These are:

   a. The preventive role which involves the examination of all persons and materiel in transit, with the aim of carrying out the tasks listed in paragraph 2 a. and b. above.

   b. The informative role, which involves the screening of all travellers with the aim of carrying out the task listed in paragraph 2 c.

11. The **preventive role** includes:

   a. Location of travel control posts. The travel control examination may take place in a building or on board ship or an aircraft. At a frontier the post should have a clear visual approach and a barrier to show the traveller where he must present himself for examination.

   b. Examination, which must take place at such a point that no person, can embark or disembark or cross the frontier without authority. Guards may be necessary. Travellers must have passports examined, visas or entry permits checked and be checked against security suspect and stop lists; they may be

interrogated to determine any security suspicions. Any security suspects will be forwarded to the interrogation centre for detailed interrogation.

c. Searches of persons and baggage and of vessels, aircraft and vehicles may be carried out.

12. The **informative role** includes the interrogation of selected travellers who have been assessed in the initial screening as possessing information of possible intelligence value. Action may consist of:

a. Obtaining the information on the spot and submitting a report or

b. Notifying the TCS HQ of the traveller's destination so that he may be interrogated by the appropriate intelligence agency.

Security Control

13. The success of travel control depends on well organized security control which, in turn, must be tied in with all other security measures. The executive responsibilities of all concerned must be clearly defined and understood.

14. The way in which traffic will be canalized through ports, frontiers or airfields will vary with the geographical and other factors. The essentials of preventive security controls are discussed in the following paragraphs.

15. **Coastlines.** A prohibited zone (PZ) is necessary, both on the seaward and landward side of the coastline. This involves a coast watching system and normal civil and service controls in the PZ. These usually consist of:

a. **Seaward side.** Movement of shipping up to a three mile limit is controlled by the Royal Navy which is also responsible for harbour control as directed by the approved port authority. Coastal vessels and small boats must also be controlled.

b. **Landward side.** A three mile limit, with restrictions of movement of all persons and vehicles in the area, will normally be imposed by the military commander in consultation with the civil authorities.

16. **Ports and dock areas.** A port of dock area will normally be declared a protected place (PP). The port commandant or approved authority is responsible for the physical protection of the port and for all other security matters therein.

17. **Frontiers.** Where no natural obstacles exist a physical barrier should be erected and the frontier clearly marked. The frontier must be guarded either by police, frontier guards or troops as a deterrent to illegal frontier crossers (IFCs).

18. A prohibited frontier zone (PFZ) may also be established to a depth of 5 - 10 miles behind the frontier. An identity check of permanent residents and authorized frontier crossers should be carried out.

19. Security along the frontier and within the PFZ is the responsibility of the area commander.

20. **Airfields.** Close liaison between air traffic control tower and TCS personnel is essential if the latter are to be informed on the movement of aircraft entering or leaving the airfield. Security control in the airfield is the executive responsibility of the station commander, advised by the I(S)O and the local APM.

Investigation of Security Control Breaches

21. Investigation must be made of all breaches of security control occurring in the PZ, PA or PP. Normally these investigations are undertaken by the Service security agencies or the civil police. TCS personnel must be kept informed of incidents of TCS interest. Only in the absence of reliable Service or civilian security agencies or police forces will TCS personnel undertake investigations themselves.

Requirements for TCS Personnel

22. To operate efficiently TCS personnel must:

a. Be trained in the principles, methods and teachings of TCS.

b. Maintain good relations with customs, police and security, embarkation staffs, port officials etc.

c. Know how to work the various technical equipment used.

d. Know shipping and airline procedures.

e. Possess a quick, balanced judgement and be capable of remembering and applying complicated regulations.

Records and Reports

23. As with all CI work the basis of TCS is a sound record and report system with a well-run central index and information database.

24. Reports will vary according to circumstances but are normally covered by standard formats. They will include:

a. Examination reports.

b. Passengers – arrivals and departures.

c. Crew report.

d. Ship report – arrivals and departures.

e. Routine intelligence reports.

f. Aliens in transit – aircraft and ships.

g. Weekly return of ships cleared.

h. Incident reports.

i. Port survey reports.

25. Records will include:

a. All necessary forms.

b. Security suspect index and database.

c. File on each ship.

d. Sufficient numbers of passes and permits in use.

e. Local index.

f. Seamen's index.

Conclusion

26. TCS is a necessary part of the overall security plan. For it to be efficient:

a. It must be integrated with the other security measures, under the control of the CI staff.

b. The executive responsibilities of all concerned, specialists and non-specialists, must be clearly defined and understood.

c. TCS personnel must be well trained in their travel control duties.

CHAPTER 15

(SPARE)

This page intentionally left blank

CHAPTER 16

NATIONAL CAVEATS

CHAPTER 16

NATIONAL CAVEATS

General

1601. This chapter provides guidance on the use of core national caveats, guidance on marking assets to be sent to the US and the special handling instructions for messages. Throughout this chapter you will see references made to the words listed below. These are deemed to mean the following:

a. "Information"- includes documents, signal messages, electronic media and any other forms of recorded information referred to in this manual.

b. “Originator”- the creator/author of the information.

c. “Owner”- the originator or his/her successor(s). In the event that the original post may have been abolished, then the owner becomes whoever has immediate line management responsibility for that post.

d. “Recipient” is a person who has entitlement to access the information.

1602. Purpose and use of national caveats. The majority of protectively marked assets are intended for dissemination in the UK, within and between government departments and agencies, and where appropriate, contractors. National caveats are available for the additional protection of sensitive assets in relation to other countries, particularly the UK’s closest allies. Assets that attract a national caveat should always be marked with an appropriate protective marking. Where necessary, a descriptor may also be applied. Any additional national caveats that may be required by originators, specifically for use within the MOD, should ensure that the same principles laid down in this chapter are applied. The core national caveats are detailed at Annex A and a summary of release levels at Annex C.

1603. Before applying a national caveat to any information, the originator should give serious consideration to the content, recipients and the likely uses to which that information will be put within MOD. This is particularly relevant in the following:

a. Organisations and training establishments where foreign exchange personnel are employed and where an inappropriate caveat could prevent foreign exchange personnel from carrying out their full range of duties in post.

b. UK industry where a high proportion of dual and foreign nationals are employed. Particularly in non-List X companies where the only MOD information held is at the non-protectively marked or RESTRICTED level.

1604. “UK” prefix. Staff should not confuse the prefix "UK" used in conjunction with a protective marking (eg UK RESTRICTED or UK SECRET) with national

caveats (eg UK EYES ONLY or UK EYES DISCRETION). The prefix "UK" **is not** a national caveat. It is used to prevent protectively marked information from being disclosed under existing or future local Freedom of Information (FOI) legislation in other countries (For sending UK information to the US see paras 1622 to 1626).

UK EYES ALPHA and BRAVO

1605. These caveats are obsolete and should no longer be used within the MOD. Although documents bearing these caveats may still be current, it is unnecessary to amend such documents retrospectively. For the purposes of releasing such information to foreign nationals you should seek advice from the originator/owner. In cases of doubt as to the protection and transmission of such documents they are to be treated as if they carry the new caveat "UK EYES ONLY" unless directed otherwise by the originator. Notwithstanding, it is important that, where access to UK EYES B material has already been agreed with the originator for foreign/integrated/attached personnel, the arrangements for such access remain extant.

UK EYES ONLY and UK EYES DISCRETION

1606. The two UK national caveats, UK EYES ONLY and UK EYES DISCRETION, should be used as follows:

a. **UK EYES ONLY.** The originator should **only** use this caveat to indicate that the information is of particular sensitivity to UK national interests. Information bearing this caveat must not be released to any foreign nationals without the originator's specific consent, as incorrect usage will cause considerable difficulties in areas where dual and foreign nationals are employed (eg such as Exchange personnel, and generally in UK industry).

b. **UK EYES DISCRETION.** The originator should use this caveat when the information, while having sensitivity to UK national interests, may be capable of wider, discretionary dissemination. In marking material with this caveat, the originator is implicitly delegating subsequent release authority to HOE/COs, who may authorise subsequent release in accordance with Annex C. This discretion provides flexibility for HOE/COs to make effective risk management decisions without reference to the originator. If in any doubt, staff should always seek advice from their Principal Security Adviser.

Composite caveats

1607. A composite caveat denotes that the information may be shared by nationals of more than one country (eg UK/US etc). The aim of composite caveats is to restrict the dissemination of sensitive assets by limiting disclosure only to foreign nationals with a proven "need-to-know", who are authorised and appropriately cleared for access. These caveats are most widely used in areas of activity where the exchange of sensitive information is routine, for example, between the international

intelligence communities. In such circumstances the need to identify to whom such information can be released is vitally important. A quick guide is given at Annex A.

Access to nationally caveated information

1608. UK nationals All UK nationals in HM Service, and MOD civilians and Service personnel who are dual nationals (of which one nationality is British), may have access to information bearing a national caveat provided the line manager is satisfied that they:

a. have a need to know the information;

b. hold a security clearance appropriate to the protective marking which accompanies the caveat (additional vetting requirements may apply to MOD civilians who are dual nationals and hold SC security clearance - see JSP 440, Volume 2, Chapter 4);

c. have been briefed on the arrangements for safeguarding such information and the local sensitivities; and

d. can otherwise be entrusted with the information.

1609. UK nationals employed in industry UK nationals employed by UK contractors may, as recipients, have access to all national caveated information. However, where MOD contracts involve the release of UK EYES DISCRETION information, which normally allows further dissemination by the recipient without reference back to the originator, the contract Security Aspects Letter should state that industry recipients may not disseminate without the agreement of the originator or owner of the information. Where no contract exists, originators should similarly qualify this requirement to recipients via an official letter.

1610. Dual nationals in industry Dual nationals (of which one nationality is British) employed by UK contractors may only have access to UK EYES DISCRETION information with approval of the originator. Where MOD contracts involve the release of UK EYES DISCRETION information, and where dual nationals have been granted access to such information by the originator, the contract Security Aspects Letter should be the same as stated in para 1609 above.

1611. Non-UK nationals in HM Service Serving members of the UK Armed Forces, who are Commonwealth or Republic of Ireland nationals, may be allowed access to UK national caveated material. This is because they are deemed to have given their allegiance to the Crown and, provided they meet the criteria set out in para 1608, are entitled to access if their duties necessitate it. However such nationals who are civilians serving within the MOD may only have access to UK national caveated material if they were already in post on 31 May 1996 (see paragraph 1632 for details). Otherwise access to composite caveated information

may only be granted, without the originator(s) approval, where the civilian non-UK national is a national of one of the countries concerned.

1612. Non-UK nationals Such nationals are not to be given access to any UK national caveated information without the express approval of the originator. They are only allowed access to composite caveated information **if** they are a national of one of the countries concerned. Release is subject to the requirements of sub-paragraphs 1608a-d above being fulfilled and having regard to the release levels set out in Table X which is issued by DESP2. Where conflict exists, the rules on release of protectively marked information take precedence.

Exchange/integrated/attached personnel (including those serving in joint operations) serving with the UK Armed Forces and Gurkhas serving in the British Army

1613. Exchange/integrated/attached personnel When planning to establish such posts in environments where there is a likelihood of unsupervised access to UK EYES ONLY material, the potential sensitivities need to be considered. If the proposed working environment cannot be managed so that such personnel are insulated from inadvertent access to UK EYES ONLY material, the agreement of all the most likely originators of such material in that environment should be obtained before the posts are established. For those personnel involved in joint operations, the advice given in Section IV to Chapter 11 should also be noted. In the case of material originating in the DIS, the single point of contact is Sec DI (Ext 86919 MB). In cases of doubt, advice should be sought from the appropriate Principal Security Adviser, who will consult DD DefSy(Info) as necessary.

1614. Gurkhas. These personnel may only have access to UK EYES DISCRETION information on a need-to-know basis.

Waivers

1615. Exceptionally, it may be necessary to grant access to a specific document to those not normally entitled to receive nationally caveated information. Permission for a waiver should always be sought from the originator, who should consider the release levels set out in Table X and consult Info(Exp)Access1 if there is potential for release under any foreign Freedom of Information (FOI) regimes. Originators are advised to consult their Principal Security Adviser before carrying out a risk analysis to determine the potential damage to UK national security should such information be passed on to a third country.

1616. Where the originator of UK national caveated information is unidentifiable, the specific authority of the Departmental Security Officer (DSO), through DD Def Sy(Info), must be sought in writing and in good time before the proposed release. The DSO will only approve release when it can be demonstrated that the originator is

unidentifiable, and will not in any circumstances override an originator's explicit decision to the contrary.

Marking, handling and transmission of nationally caveated information

1617. Nationally caveated information must always be marked with an appropriate protective marking, and, when necessary, a descriptor. The sequence of these markings should be protective marking, descriptor and national caveat.

1618. National caveats must not appear on envelopes. You should address it to either an individual or a specific post entitled to receive it. The envelope should be marked EXCLUSIVE. This will ensure that in an addressee's absence, special local arrangements will enable a designated officer to gain access to the information and act accordingly. Details on how to correctly despatch protectively marked information is given in JSP 440, Volume 1, Chapter 4.

1619. Registered files, branch folders or other covers enclosing caveat information must be marked accordingly. When in transit, despatching procedures laid down in JSP 440, Volume 1, Chapter 4 are to be followed.

1620. Originators should, when asked to permit discretionary access to caveated material by those not normally entitled to see it, consider if access can be limited to a single document rather than allow full access to a range of assets. This is particularly important in cases where information is stored on and accessed from IT systems. Such access will be subject to appropriate access controls and user profiles for IT systems.

1621. Guidance on distributed IT systems and the interconnection of IT systems is provided in JSP 440, Volume 3 - Information Technology. The System Security Policy will ensure that information attracting a national caveat can only be accessed by either those who satisfy the requirements of paragraph 1608 above or nationals of other countries to which the caveat authorises release.

Protecting information to be sent to the US

1622. The United States has operated a FOI regime for some years under the US Freedom of Information Act (US FOIA). Great care must be taken when sending information to the US to guard against the risk that UK information, which would be exempted from disclosure requests under our own legislation, could be released on application to the US.

1623. Under the terms of the UK/US General Security Agreement, UK protectively marked material will be protected form automatic release, provided that it is prefixed "UK". However, such information may still be requested under US legislation, and originators should be prepared to justify why the information should not be

disclosed, quoting the UK FOI exemption when necessary. Furthermore, where it is necessary to limit dissemination of sensitive information beyond a US authority holding the UK-sourced data, in addition to the appropriate protective marking, the document should be clearly marked with the precise conditions for its disclosure to other authorities, and for any public release.

1624. UK information without protective markings (ie UNCLASSIFIED) will be more vulnerable to applications for disclosure under US FOIA. However, the recent Presidential Executive Order (EO) 12958 has made some provision for protecting UK UNCLASSIFIED information, although this will only apply to UK information that would also be exempted from the provisions of UK FOI 2000. US Department of Defense (DoD) staff advise that one or other of the labels, shown at Figure 1a or 1b below, should be used as appropriate to denote material requiring protection from public disclosure:

Use either of the following as appropriate:

This document contains sensitive information of the UK Government which is withheld from public disclosure in the United Kingdom and is provided to the United States Government on the condition that it is not to be released to the public until [insert date for release]

Fig 1a

This document contains sensitive information of the UK Government which is withheld from public disclosure in the United Kingdom and is provided to the United States Government on the condition that it is not to be released to the public without the approval of the UK Government.

Fig 1b

It should be noted that this label will only provide protection to information passed to the US Departments of Defense and Energy, as they are the only departments granted exemption from the US FOIA provisions. No other marking should be used unless there is a written agreement with the US authority concerned that information so marked will be protected from disclosure.

1625. The US authorities do not recognise the UK term "protective marking", instead using the term "classification". Furthermore, the UK's "RESTRICTED" classification is not recognised in the US. In accordance with EO12958, information marked UK RESTRICTED will be treated as classified information by the US recipient. Upon receipt, it will be marked on the cover or first page with, "This document contains UK RESTRICTED information; to be protected in compliance with EO 12958". US documents, or other media containing UK RESTRICTED information will also be marked with this wording. Additionally, each separate paragraph or segment will be marked to denote the UK RESTRICTED content of the information (shown as 'UK_R').

1626. MOD staff originating information which incorporates US-sourced material should contact the relevant US DoD desk officer to determine whether or not the US-sourced content is sanctioned for release under the US (or any other) FOI legislation **before** it is issued. If MOD staff are unable to identify the US source of origin, they should contact Info(Exp)-Access staff who will try and locate the appropriate US DoD desk officer for advice.

1627. Originators are encouraged to mark individual paragraphs of documents with the appropriate protective marking as this will greatly assist in assessing information which have been requested for release under any FOI legislation. Originators should consider especially:

a. Has the appropriate protective marking been used?

b. Is the document likely to be released to foreign governments now or in the foreseeable future?

c. Is the sensitive element of the document clearly identifiable?

1628. Departments and agencies should consult their Principal Security Adviser where they experience difficulties in applying appropriate markings for assets to be sent to the US, or in the general handling of US classified information.

Formal messages bearing a core national caveat or special handling (SPH) instructions

1629. Formal signal messages and diplomatic telegrams bearing any of the core national caveats (see Annex A to this Chapter) or a Special Handling (SPH) instruction (see below), are given 'special handling' by appropriately cleared communications staff. Caveats and SPH instructions are entered in the 'Special Handling Caveat/Descriptors' box or field on the message form and, with the exception of 'UK COMMS ONLY', as the first words in the message text. Messages containing a caveat or SPH instruction are to bear an appropriate protective marking for caveats and SPH instructions, and the control Subject Indicator Code (SIC) AAA followed by appropriate SIC(s). The term 'special handling' (SPH) embraces caveats and SPH instructions.

1630. Originators may specify that a signal message receives SPH by assigning a SPH instruction or caveat. Not all SPH instructions are recognised by the international community - this is indicated in brackets after each instruction shown below.

a. **EXCLUSIVE** (Internationally recognised). 'EXCLUSIVE' is applied to messages which may only be seen by specified individuals or their nominated representatives. The words 'EXCLUSIVE FOR.....FROM.....' are entered as the first words of the text.

b. **DELTEXT** (UK Services only - to be used with a UK protective marking). 'DELTEXT' is used where the content of a message is particularly delicate or sensitive and its handling and distribution has to be strictly limited. 'DELTEXT' is entered as the first words of the text.

c. **UK COMMS ONLY** (UK Services - to be used with a UK protective marking). UK protectively marked messages may, under certain circumstances, be routed over non-UK networks and may consequently be read in clear by non-UK personnel. 'UK COMMS ONLY' is used when an originator considers it essential that a signal is seen and handled only by UK comms staff and is routed accordingly. This instruction is to appear in the Special Handling Caveat/Descriptor box or field but is not entered at the start of message text. Further guidance on the use of 'UK COMMS ONLY' is given in Annex B.

1631. The changes to security described in this chapter, and the wider distribution of SPH cryptographic facilities, has enabled caveats and SPH instructions to be sent and received in signal form throughout Defence.

a. COMMCEN staff can advise on the handling, delivery and collection of SPH messages.

b. Caveats are not to appear on outer envelopes, (see paragraph 1618). Except where a COMMCEN is in the same building as the recipient or addressee, such messages are always to be double enveloped. Details of COMMCEN SPH procedures are contained in ACP 122 UK Supp-1 (Communications Security).

c. The use of SPH cryptographic keying material and authentication tables is detailed in BRN/09/2 and BAA/09/2.

Changes to the nationality rules

1632. On 1 March 1996 the Government announced changes to the nationality rules for recruitment to the Civil Service. As a result, from 1 June 1996 Irish and Commonwealth citizens will no longer be eligible for recruitment to "Reserved" posts. These are posts that require special allegiance to the state and which in future will be reserved for UK nationals. However, Irish and Commonwealth citizens in post on 31 May 1996 will have reserved rights to the full range of posts for the remainder of their careers, provided that there is no break in service. These new rules should be borne in mind when deciding whether or not a person should have access to caveated information.

ANNEX A TO CHAPTER 16

CORE NATIONAL CAVEATS

Core national caveats	Release to nationals of				
	United States	Canada	Australia	New Zealand	Other Countries
UK EYES ONLY	No	No	No	No	No
UK EYES DISCRETION [1]	No	No	No	No	No
UKUS EYES ONLY	Yes	No	No	No	No
CANUKUS EYES ONLY	Yes	Yes	No	No	No
CANAUSUKUS EYES ONLY	Yes	Yes	Yes	No	No
CANAUSNZUK EYES ONLY	No	Yes	Yes	Yes	No
CANAUSNZUKUS EYES ONLY [2]	Yes	Yes	Yes	Yes	No
AUSNZUKUS EYES ONLY	Yes	No	Yes	Yes	No
AUSUKUS EYES ONLY	Yes	No	Yes	No	No

Notes:

1 See Annex C for release of UK EYES DISCRETION information to exchange and integrated officers and officers on attachment with the MOD.

2 In certain arenas, primarily the intelligence domain, the exchange of information with all of the allies mentioned in the table above is routine. In such circumstances, it may be a branch's/unit's or agency's normal, authorised practice to allow the holders of information discretion to share it with those countries, with the caveat CANAUSNZUKUS EYES ONLY being assumed rather than explicit. Originators should therefore ensure that they apply the appropriate national caveat to information when it is necessary to constrain dissemination to nationals of those countries.

This page intentionally left blank.

ANNEX B TO CHAPTER 16

UK PROTECTIVE MARKINGS IN MESSAGES TO ADDRESSEES SERVED BY NON-UK COMMS NETWORKS AND USE OF THE SPH INSTRUCTION 'UK COMMS ONLY'

Introduction

1. The SPH instruction 'UK COMMS ONLY' may be appropriate for example where a UK addressee is served by a non-UK comms network, and sight of the text of a message may cause embarrassment to either the UK or the host organisation/nation. The use of this SPH instruction ensures that a message reaches the intended UK addressee(s) without having been seen by non-UK nationals. (This may be achieved by off-line encryption, by using suitably approved or protected UK communications links or, in some cases by sending a signal by protectively marked mail.) The paragraphs below contain the rules for the highest UK protective markings which may be sent over non-UK communications networks.

UK protectively marked messages to UK authorities served by non-UK comms networks

2. Originators should use the following information as a guide to when to use 'UK COMMS ONLY'.

a. **NATO networks.** Messages up to and including RESTRICTED may be sent in clear over suitably protected or approved NATO networks.

b. **AUS/CAN/NZ/US networks.** Messages up to and including RESTRICTED may be sent in clear over suitably protected or approved AUS/CAN/NZ/US circuits. Exceptions are currently granted for the following:

(1) NP 1011 - up to and including CONFIDENTIAL, (served by the US network).

(2) RNLO DIEGO GARCIA - up to and including CONFIDENTIAL, (served by the US network).

(3) HM SHIPS/RFAs reading AUS/CAN/NZ/US broadcasts - up to and including CONFIDENTIAL in clear.

c. **Other Foreign networks.** Messages up to and including RESTRICTED may be sent in clear over suitably protected or approved foreign

networks.

UK protectively marked messages to foreign agencies only.

3. Provided the address section does not include a UK Signal Message Address (SMA), signal messages up to and including UK SECRET may be sent to foreign agencies over suitably secure and approved US, NATO or old Commonwealth networks. Originators must be sure the text is releasable, and must insert the words 'UK CLASSIFIED RELEASE IN CONFIDENCE' at the start of message text.

UK protectively marked messages addressed to UK authorities and foreign nationals

4. Provided the information is releasable to the foreign addressees concerned, messages to both foreign agencies and UK addressees (in the same message) protectively marked up to and including UK SECRET, may be sent in clear over suitable secure and approved US, NATO or old Commonwealth networks. Originators must insert the words 'UK CLASSIFIED RELEASE IN CONFIDENCE' at the start of message text.

Example of a UK SECRET message sent to foreign agencies and UK addressees

5. The address section and start of text of a UK SECRET message to UK addressees and foreign agencies served by more than one foreign network.

FROM HQ STC		(DCN)
TO	DEFAIR AFSA	(Australian network)
	BRITMILREP CANBERRA	(DCN)
INFO	RAF MARHAM	(DCN)
	DIA WASHINGTON	(US network)
	DPA CAPE CANAVERAL	(US network)

SECRET. HKL. UK CLASSIFIED RELEASED IN CONFIDENCE.

Note. Had the above message been addressed to UK addressees only, UK RESTRICTED would be the highest protective marking that could be sent in clear over foreign networks.

ANNEX C TO CHAPTER 16
SUMMARY OF RELEASE LEVELS

CORE NATIONAL CAVEATS	UK NATIONALS	DUAL NATIONALS IN HM SERVICE	DUAL NATIONALS IN UK INDUSTRY	NON-UK NATIONALS # IN HM SERVICE	NON-UK NATIONALS	EXCHANGE/ INTEGRATED/ ATTACHED PERSONNEL AND GURKHAS
UK EYES ONLY	YES	YES (DV/SC+)	NO	YES (DV/SC+)	NO	NO
UK EYES DISCRETION	YES*	YES (DV/SC+)	YES*	YES (DV/SC+)	NO	YES
UK/US EYES ONLY	YES	YES (DV/SC+)	NO	NO[o]	NO[o]	NO[o]
CANUKUS EYES ONLY	YES	YES (DV/SC+)	NO	NO[o]	NO[o]	NO[o]
CANAUSUKUS EYES ONLY	YES	YES (DV/SC+)	NO	NO[o]	NO[o]	NO[o]
CANAUSNZUK EYES ONLY	YES	YES (DV/SC+)	NO	NO[o]	NO[o]	NO[o]
CANAUSNZUKUS EYES ONLY	YES	YES (DV/SC+)	NO	NO[o]	NO[o]	NO[o]
AUSNZUKUS EYES ONLY	YES	YES (DV/SC+)	NO	NO[o]	NO[o]	NO[o]
AUSUKUS EYES ONLY	YES	YES (DV/SC+)	NO	NO[o]	NO[o]	NO[o]

Notes:

* Within industry, may only be released to named recipients, and not disseminated further without the agreement of the originator of the material – see paras 1609 and 1610 respectively.

° Non-UK nationals may only be granted access without the originator's permission if they are a national of one of the countries concerned.

Serving members of the UK Armed Forces and MOD civilians who are Commonwealth or Republic of Ireland nationals – see para 1611.

+ Additional vetting requirements may apply to MOD civilian dual nationals holding an SC clearance.

CHAPTER 17

STRAP SECURITY GUIDELINES (SANITIZED)

This page intentionally left blank.

CHAPTER 17

STRAP SECURITY GUIDELINES (SANITIZED)

Introduction to the STRAP System

1701. The "STRAP System", which is explained fully in Volume 5 - STRAP Security, is a set of nationally agreed principles and procedures to enhance the "need-to-know" protection of sensitive intelligence (and related operational information) produced by the principal UK Intelligence Agencies, including MOD sources. STRAP is a Codeword, not an acronym. It is used to mark most types of material handled under the STRAP System. (Where this is practicable, because of technical constraints, the originating Agencies will give guidance on the STRAP equivalent of Codewords.) The Codeword STRAP, in isolation, does not require a protective marking.

The Threat to Sensitive Intelligence

1702. The principal threat to sensitive intelligence arises when a target becomes aware of an intelligence attack. So warned, the target can initiate countermeasures, and intelligence of the kind protected by the STRAP System is particularly vulnerable to this type of reaction.

1703. The UK's intelligence capability is similarly at risk when knowledge of an intelligence success against a target falls into the hands of any other country, organisation or individual. They may assume their own activities against the UK national interest to be similarly targeted. At worst, future success against a valuable target could be denied, and an agent's life lost, but in any event, the cost of recovering lost intelligence capability is likely to be very high.

1704. The "traditional" threat to the UK's intelligence operations from foreign intelligence services (FIS) remains a potent one - particularly in the field of scientific, technical and industrial espionage - and the classic methods of attack are likely to be employed. However, many of today's high priority intelligence targets are not connected to a foreign Government or, therefore, to a professional intelligence service. Whilst this may be seen to reduce the level of risk, it does not make these intelligence operations any less vulnerable.

1705. For example, activities against the UK national interest, such as terrorism, drug trafficking and other illegal dealing by individuals and organisations are increasing in significance - and hence in priority as intelligence targets. The threat to operations against these targets is less likely to arise from positive acts of counter-espionage, than from leakage of information through disaffected members of staff, or as a result of the attentions of an investigative journalist, or simply by accident or carelessness.

1706. In this wider definition of Threat, the "enemy" is unwelcome publicity of any kind, and through any medium. The most effective safeguard is to reinforce those

aspects of security that minimise the risk of leakage of sensitive intelligence operations or product into the public domain - whether by accidental exposure or deliberate intent. The STRAP System aims to achieve this.

How the STRAP System Operates

1707. The STRAP System seeks to "add value" to the standard security measures employed for intelligence matters (TOP SECRET, SECRET etc), by using additional effective procedures. It aims to minimise the risk of unauthorised disclosure of particularly vulnerable intelligence assets by:

a. restricting access to sensitive intelligence material on a strict "need-to-know" basis;

b. agreeing the appropriate facilities for its protection in transit (ie "STRAP Channels") use, storage and disposal; and

c. providing explicit briefings and guidance for individuals who handle this type of material.

1708. Information that requires protection under the STRAP System will be clearly defined and labelled. It will be carried by authorized couriers during transit, and signed receipts will be obtained at all stages of handover.

Three Levels of Protection

1709. Within the overall definition of "particularly sensitive", some items of intelligence, handled within the STRAP System, require more stringent protection than others. In order to avoid being over restrictive, material is assigned, by the originators, to one of three "levels" of STRAP protection (or"handling"). These are designated, in ascending order of sensitivity and, hence, access control: STRAP 1, 2 or 3.

Administration of the STRAP System

1710. DDef Sy is responsible overall for the administration of the STRAP System within the Department. He is a member of the STRAP Management Board which has overall responsibility for the review and formulation of STRAP policy and guidelines. Any queries regarding the Department's policy on STRAP should, in the first instance, be referred to:

Departmental Policy - InfoSy(Pol)1, Main Building
Tel: 020 7218 3994

1711. Within the Department are individually appointed STRAP Security Officers (STRAPSOs) who oversee the implementation of the approved STRAP security measures within the Services and MOD HQ, DPA and DERA. The principal Sector STRAPSOs are as follows:

Royal Navy	-	DNSyICP.X3 SCU Leydene Tel: 01730 824205/6
Army	-	DI(SI) SO2 (S) Old War Office Tel: 020 7218 3989
Royal Air Force	-	SyCIS3b(RAF) RAF Brampton Tel: 01480 52151 Ext 6667
MOD HQ, DPA & DERA	-	DIS Sy(STRAPSO) Old War Office Tel: 020 7218 6141/85030/82608

Inadvertent Access to STRAP Material

1712. Anyone not cleared to receive material or information marked with a STRAP label, who inadvertently gains access, must not show it or discuss it with anyone else, but should immediately report the fact to one of the principal Sector STRAPSOs listed in paragraph 1711 above. Arrangements will then be made for the safe custody of the material by the relevant STRAPSO. You will be briefed on the fact that the material is sensitive intelligence material and that you are obliged not to divulge any knowledge you may have gained through inadvertent access.

Relationship with STRAP Authorities

1713. The arrangements described in the foregoing paragraphs, which are common to all Government Departments, are codified by a Service Level Agreement (SLA) between the Department and the STRAP Authority. The SLA between MOD and the STRAP Authority is signed by AUS(S&S) (now DGS&S), as the Departmental Security Officer, and the Chairman of the STRAP Management Committee. Detailed arrangements for procedure applicable to each Sector under the overarching SLA, are contained in Annexes to the MOD SLA. Copies of these are held by Principal Security Advisers.

This page intentionally left blank.

CHAPTER 18

SECURITY INSTRUCTIONS FOR THE USE OF UNARMED COMMERCIAL GUARD FORCES IN GREAT BRITAIN

CHAPTER 18
SECURITY INSTRUCTIONS FOR THE USE OF UNARMED COMMERCIAL GUARD FORCES IN GREAT BRITAIN

Introduction

1801. The purpose of these instructions is to set out minimum security standards, criteria and procedures for the selection and use of commercial companies to provide contracted unarmed guard forces to the MOD, including its agencies. Heads of Establishment (HOE) may seek higher standards if they wish, bearing in mind the additional costs which might be incurred.

1802. When an establishment is considering the employment of a Commercial Guard Force (CGF) or is considering the renewal of an existing CGF contract the HOE is to inform the appropriate PSyA. Contact details are at Annex A. Advice on the Sequence of Events to be followed during this process is at Annex B. The responsibilities of Heads of Establishment and advice for staff are set out in Annex C and its appendices. (Appendix 1 details the Daily Briefing to be given to guards, Appendix 2 gives advice on how to monitor guard force performance and Appendix 3 summarises the vetting requirements for commercial guards).

1803. CGF may be used, where appropriate, by MOD establishments in Great Britain subject to the MOD Guard Service (MGS) retaining 75% of all unarmed civilian guarding posts within the Defence Estate. This condition was established in an undertaking by Ministers given to the House of Commons Defence Committee (HCDC Session 1995-96, Eighth Report) and is to be kept under review by the PSyA and D Def Sy who maintain a database of commercially contracted guard forces. Should a proposed commercial contract appear to lead to a breach of this undertaking, Ministers will be informed by DG (S&S); their agreement is to be obtained before the relevant contract is awarded. The future of the ratio, and the current embargo on further CFQ of contract guarding imposed by Minister (AF) in 1998 is to be determined after consultation with Ministers.

1804. One of the HCDC recommendations, accepted by Ministers, enabled MGS to compete with the private sector at contract re-let (provided bids were mounted under Competing for Quality (CFQ) rules) and to compete for sub-contracts to prime contractors on multi-activity contracts.

1805. No contract for the use of commercial guards may be entered into before consulting the PSyA. Contracts are to be arranged through the appropriate Commercial Staff (CS). Contact details are at Annex A.

1806. Guidance for the HOE, the PSyA and CS on the security aspects of seeking a commercial guarding contract is set out at the Annexes. The guidance applies to the security element of all guarding contracts, including multi-activity contracts (MAC), public and private partnership projects involving guarding, private finance initiatives, market testing, contracting out processes and to sub-contractors providing a guarding service via a prime contractor. The decision whether to include security guarding in a MAC is to be a matter of consultation with DGS&S through D Def Sy.

Categorisation of establishments and composition of guard forces

1807. Details of categorisation of Defence Establishments for guarding purposes and composition of guard forces are in JSP 440 Volume 1, Chapter 5, Section VIII. Details of Categorisation for general security purposes are at JSP 440 Volume 1,Chapter 2, Paragraph 0214a. PSyAs are to take into account these instructions when determining whether use of a CGF is appropriate. CGF may be used on any unarmed guarding task. They may be integrated with armed guard forces (e.g when armed guarding is required MDP or service personnel may provide the armed element supplemented by a CGF to carry out unarmed tasks). The use of CGF in Category A establishments must be carefully considered, with due regard being paid to the tasks the CGF will be required to undertake and the appropriate levels of security clearance required.

1808 to 1809. *Spare*

Criteria for selecting a commercial guarding company

General

1810. To ensure that MOD contracts are only awarded to CGFs that are capable of achieving and sustaining the required standards, the compulsory eligibility criteria set out in Paragraphs 1811 to 1817 are mandated. Under CFQ rules MGS are exempt from this scrutiny.

Membership of professional bodies

1811. Companies are to be selected from among those:

a. Registered on the DTI UK Register of Quality Assured Companies

or

b. The Inspectorate of the Security Industry's Register of Manned Security Companies.

PSyAs and CS hold copies of these registers.

Accreditation

1812. Companies which are invited to tender must satisfy the CS that they are certified by an accredited third party body to ISO 9000 sequence of Quality Management and Quality Assurance Standards. It is important that the Certification Body also includes in its accredited scope, the full requirement of BS 7499:1998 (Code of Practice for Static Guarding, mobile patrol and keyholding services). Particularly stringent attention must be paid to the company's recruiting policy and standards.

Structure and Management

1813. The PSyA should take the following steps in consultation with CS:

a. If necessary confirm with D Def Sy and with HOEs, at whose sites the firm has an existing contract, that contracts and are being fulfilled satisfactorily.

b. Firms tendering for the first time should be assessed as to their suitability to hold the proposed contract, by inspection against the criteria laid down in these instructions. The PSyA should pass this information to the CS.

Manpower

1814. The CS is to ensure that the contract stipulates that, in accordance with the EU Working Time Directive, guards are to work a maximum average 48-hour week, in shifts not exceeding 12 hours. A minimum manning ratio of 4 guards for each 24-hour post is mandated. The Contractor is to maintain an adequate pool of employees who are security cleared and trained to the required standards to ensure that the guarding requirement is fully met at all times.

Training

1815. Companies invited to tender must agree that all commercial guards and on-site supervisors will have achieved the training standards laid down in Annex D, before the start of the contract.

Statements of requirements

1816. Advice on the need for and preparation of Statements of Requirements (SOR) is at Annex E.

Vetting

1817. All commercial guard force personnel must undergo a Basic Check (BC) and Counter Terrorist Check (CTC) before they are permitted to take up their duties. The

procedure to be followed, including completing identity verification, is contained at Appendix 3 to Annex C. Instructions for the vetting of Commercial Guards are contained in JSP 440, Volume 2, Chapter 10.

Evaluation of tenders

General

1818. On receipt of tenders, CS will call for a technical evaluation. The purpose of the evaluation is to ensure that the company meets the standards required by these instructions. It is to be conducted by the PSyA on behalf of the HOE. The PSyA is to inform the CS of any company judged unable to meet the security requirements of the Contract. The report of the Technical Evaluation should be forwarded to the CS who will then conduct the commercial evaluation and, taking all aspects of the tender into account, recommend a company to the HOE for award of the contract.

Medical

1819. In putting forward the name of a Guard or Supervisor for employment the Contractor should be required to confirm in writing in each and every case that they have established that the Guard or Supervisor is medically fit for employment. If this is subsequently found not to be so, the Guard or Supervisor should be withdrawn by the Contractor and replaced by an approved substitute. The cost of any medical examinations required should be borne by the company competing for the Contract. The medical standards required by a company of its site employees should be examined. The following is an extract from BS 7499:1998. Paragraph 5.1. These should be used as medical guidelines when drawing up a contract.

"Persons [potential employees] should present a medical history prior to commencement of employment, and should demonstrate general good health and mobility by undergoing physical tests. Eyesight, hearing and sense of smell should be checked.

Procedures should be in operation to ensure that the physical condition of persons is maintained during the length of employment. If there is a change in a person's duties, further physical tests should be performed by the person if appropriate. Persons employed for security duties should be aged between 18 years and 65 years. Persons over 65 years should undergo annual medical examinations to ensure fitness for duty."

Conduct

1820. A code of conduct for on-site employees, the terms of which tendering companies must accept, is at Annex F.

Security consideration on commercial issues

1821. Advice to CS on the security considerations in certain commercial issues is at Annex G.

This page intentionally left blank.

ANNEX A
COMMERCIAL STAFFS AND TLB PRINCIPAL SECURITY ADVISERS

COMMERCIAL STAFFS

1. **CINCFLEET / 2SL/CNH:**

   a. CB/FLEET 1F, Spur 4, the Crescent, , Ensleigh, Bath, BA1 5AB.

   b. Tel: 01225 467074 (Bath/Ensleigh Ext 67074)

   c. Fax: 01225 468761 (Bath/Ensleigh Ext 68761)

2. **CINCLAND / AG:**

   a. DD/LCCS, G9, HQ LAND, Erskine Barracks, Wilton, Salisbury, Wilts, SP2 0AG

   b. Tel: 01722 433137 (Salisbury Mil, Ext 3864)

   c. Fax: 01722 433142 (Salisbury Mil, Ext 3142)

3. **CINCSTC / HQ PTC:**

   a. ADC/STC, Bldg 1406, RAF Daws Hill, High Wycombe HP11 1SH

   b. Tel: 01494 461461 Ext 5379/5308/5380 (High Wycombe RAF, Ext 5379/5308/5380)

   c. Fax: 01494 461461 Ext 5094/5399 (High Wycombe RAF, Ext 5094/5399)

4. **MOD Centre TLBs and Defence Estates:**

   a. CB (Com) 1, Central Budgets Commercial, Room 311, Wellesley House, 103-109 Waterloo Street, Glasgow G2 7BN.

   b. Tel: 0141 224 8328 (Glasgow Mil Ext 8328)

   c. Fax: 0141 224 8412 (Glasgow Mil Ext 8412)

5. **Defence Procurement Agency (DPA):**

   a. FMG1b1, Poplar minus one, Mail Point # 2005, Abbey Wood, Bristol, DS34 8JH

   b. Tel: 0117 91 #30627

   c. Fax: 0117 91 #30926

PRICIPAL SECURITY ADVISERS

TLBs

6.	CINCFLEET / 2SL/CNH	01705 727131
7.	CINCLAND / AG	01722 336222 #2349
8.	CINCSTC / HQ PTC	01494 461461 #6364
9.	PJHQ	01923 826161 #46145
10.	CDL (DLO)	01225 468712 / 467772
11.	CDP (DPA)	0117 9130627
12.	MOD Centre	0207 2180963

Trading Funds

DERA	01252 397272 (until 1 Jul 01, when **DERA** becomes **QinetiQ** and ceases to be a Trading Fund)
DSTL	01980 613424
Meteorological Office	01344 854631
UK Hydrographic Office	01823 337900 # 3363
DARA (via DLO)	01225 68712 67772

ANNEX B

SEQUENCE OF EVENTS IN APPOINTING COMMERCIAL GUARD FORCES

1. The Head of Establishment (HOE) informs the appropriate Commercial Staff (CS) and the TLB Principal Security Adviser (PSyA) that the employment of a Commercial Guard Force (CGF) is being considered.

2. Having received confirmation from the PSyA that the award of a commercial guarding contract would be compatible with current security policy the Head of Establishment (HOE) decides if such a contract is desirable. The establishment then initiates a Statement of Requirement (SoR) as detailed at Annex D.

3. The HOE informs Trade Unions. The consultation procedures contained in the MOD Personnel Manual, Volume 12, Chapter 3, Annex G should be followed. If MOD permanent staff are to be transferred under the Transfer of Undertakings (Protection of Employment) Regulations 1981 (TUPE), advice is to be sought from Agency / TLB secretariats as appropriate.

4. The PSyA approves SoR.

5. SoR sent to finance branch for endorsement.

6. Financially endorsed SoR sent to CS.

7. CS advertises in Contracts Bulletin. Conduct pre-qualification exercise. CS issues the Invitation to Tender (ITT) to firms who meet the criteria laid down in these instructions. A copy of the ITT is to be sent to HOE and PSyA. No more than six firms will be invited to tender and CS will take other steps to shorten the list if more than six firms pre-qualify.

8. Site Meeting to be organised by HOE; representatives of the PSyA (usually represented by their inspection/auditing organisation (Area Security Team (RN), 2 MI Bn (Army), P & SS (RAF) or CB (Sy) (Centre)), tendering companies and CS attend.

9. Tenders received by CS.

10. CS forwards the technical element of the tenders to HOE (through the Project Officer undertaking management of the requirement on his behalf) and the PSyA for evaluation. The PSyA is to carry out this evaluation and inform CS of any tenders that are non-compliant and ranking all tenders in order of technical merit.

11. CS conducts commercial evaluation of tenders, and taking into account the technical and commercial evaluations, recommends the winning tender to the HOE for approval.

12. Finance branch approves funding for the Contract.

13. CS awards contract.

14. CS forwards full detail of Contract to the HOE.

15. CS notifies D Def Sy and the PSyA of details of winning bid using the proforma at Annex H.

16. Contractor initiates vetting action for his employees in accordance with Annex C, Appendix 3.

ANNEX C

RESPONSIBILITIES OF HEADS OF ESTABLISHMENTS

Acquiring a Contract

1. On reaching a decision that contract guarding for the establishment is desirable, the Head of Establishment (HOE) is to nominate a Project Officer from the staff, directed to manage the project from "cradle to grave". The Project Officer is to establish contact with the Principal Security Adviser (PSyA) and Commercial Staff (CS). Some PSyAs may direct the DO to establish contact and maintain liaison with the local Security Unit. The PSyA will provide contact details.

2. The Project Officer is responsible, on behalf of the HOE, for the following:

   a. In consultation with the PSyA and CS, preparing a Statement of Requirement (SoR) for the required guarding service.

   b. In conjunction with the PSyA, acquiring financial endorsement for the SoR from the appropriate budget holder.

   c. In conjunction with the PSyA and CS, briefing prospective contractors on site as to the requirement.

   d. In conjunction with the PSyA, conducting a technical evaluation of the tenders.

   e. In consultation with the CS, acquiring financial approval for the selected Contract from the appropriate budget holder.

   f. In conjunction with the Establishment Security Officer, processing the security clearances for the Contractor's employees.

Supervising the Contract

3. The HOE is to appoint a Designated Officer (DO) to supervise the contract. The DO is to hold a copy of the Contract and is to be the single point of contact for the CS and PSyA with regard to all on-site aspects of the Contract.

4. In supervising the Contract at local level, the DO is responsible for the following:

a. Establishing contact with the Contractor's contract manager and arranging a timetable of formally recorded meetings to discuss the working of the Contract.

b. Establishing contact with the Contractor's local on-site supervisor and arranging a procedure for briefing and discussion on day-to-day working of the Contract.

c. In consultation with the CS, establishing an agreed procedure with the Contractor for auditing Performance Indicators set out in the Contract; conducting the periodic audit and reporting findings to the PSyA and CS.

d Maintaining an establishment incident log to record any shortcomings by the Contractor's employees; this log to be the basis for discussions with the Contractor's local supervisor and contract manager.

e. Reporting to the PSyA and CS any shortcomings that cannot be resolved at sub-para d above.

5. Further detailed guidance for the DO in respect of his responsibilities in supervising the contract is set out in the Appendices to this Annex.

APPENDIX 1 TO
ANNEX C

DAILY BRIEFING FOR GUARD FORCE

1. Every member of the guard force is to be briefed by his supervisor, who will, in turn, have received a briefing from the establishment DO or his representative, before the tour of duty starts.

2. The briefing should include at least the following as appropriate, but it should be noted that this list should not be regarded as exhaustive:

a. Changes to the threat.

b. Alert state.

c. Changes to the normal routine.

d. Planned events.

e. Details of known visitors, special events etc.

f. Specific areas of responsibility e.g.:

(1) Passes (personnel/vehicles).

(2) Vehicle search.

(3) Enforcement of parking restrictions.

(4) Contractors employees/vehicles.

(5) Security of buildings.

g. Details of armed patrols.

h. Communications.

i. Administration.

This page intentionally left blank.

APPENDIX 2 TO ANNEX C

MONITORING GUARD FORCE PERFORMANCE

General

1. This Appendix gives guidance to the Designated Officer (DO) in monitoring Commercial Guard Force performance. In order to exercise any control of performance it is incumbent on the Head of Establishment (HOE) to ensure that the following points are covered fully in the Statement of Requirements (SoR) - (see Annex E).

2. The DO is responsible to the HOE through the Project Officer for maintaining a record of contract performance (See Annex G, Paragraph 7 for the action to be taken in the event of unsatisfactory performance). The following aspects are to be covered:

a. Professional performance against the requirement stated in the Contract including a record of quantifiable performance indicators.

b. The scale and frequency of deficiencies.

c. Training standards.

d. The turnover of guards.

e. Administrative performance - relevant aspects are: freshness, smartness, state of the uniform, reports of breaches, log sheets, discipline and fitness for work generally, including training.

f. The quality of supervision by the Contractor, both at local level and at company management level and responses to any establishment complaints.

Manpower

3. The Contractor should maintain sufficient resources to ensure the performance required in the contract is achieved. This may include maintaining a specified number of guards on site at times of designated alert.

4. In nominating those staff that he would wish to assign to the task, the Contractor must provide a strength of Guard Force sufficient to be self-contained and able to cover normal time off, meal breaks, leave, training and sickness. The mandated minimum ratio is 4 guards to each 24-hour guard post.

5. To cover exceptional circumstances such as long-term sickness or non-arrival of staff for duty and to ensure that only a maximum of 56 hours a week is

worked, (see Paragraph 9 below) the Contractor should be required to nominate reserves; these reserves, to be approved by the DO, must have successfully completed the MOD Unarmed Guard Training Course; the induction element of the course must have been completed within the preceding 12 months at the site where the guard is to be employed. If it has not the training must be given. Reserves may be employed elsewhere within the company, but their use on the DO's task, although exceptional, must have priority if and when the need arises. These nominated reserves should be on 2 hours notice to be on site for duty; reserves should also be nominated on a ratio of one for every 6 persons employed for guarding tasks in the Contract. The provisions of the Contract must apply to proposed replacement staff as they apply to other staff.

7. The Contractor should be required to take all reasonable steps to avoid changes in staff assigned to and approved for the guard force. Where the Contractor proposes such a change, the DO should be given not less than one month's notice thereof. If circumstances wholly beyond the Contractor's control prevent the giving of such a period of notice, the Contractor should be required to give the maximum period of notice possible.

Hours of work

8. The DO should ensure that any contractual limitations on working hours are adhered to. A daily record is to be kept on site by the Contractor for the regular inspection by the DO, of hours and shifts worked by each individual.

9. DOs should be aware that the normal hours of work should be 48 hours per week; as an exception an extra shift or number of hours may be worked up to a maximum of 56 hours in a period of 7 days. A Guard or Supervisor, having worked 56 hours in 7 consecutive days, must be given 48 hours consecutive time off by the Contractor unless there is an emergency whilst he is waiting for a replacement. Over an agreed reference period, normally 17 weeks but in certain circumstances (as set out in the EU WTD) up to 52 weeks, the contractor is to ensure that his employees do not exceed an average of 48 hours of weekly working time.

10. Whenever a Guard or Supervisor leaves his post (e.g. for a rest, meal or tea break) the contract should require his duties to be assumed by a replacement guard or supervisor.

Staff clothing and equipment

11. **Clothing**.

a. The Contractor shall ensure that each guard or supervisor accepted by the DO for employment is dressed in a clean, presentable and military style uniform (including head wear) and that he has stout, clean footwear. The uniform is to be approved by the DO in accordance with Section 2 of the Uniforms Act 1984.

b. The Contractor shall further provide foul weather clothing for each Guard and Supervisor when on duty which, when worn, will not impede the execution of their tasks.

12. **Equipment**.

a. The Contractor shall provide for each guard or supervisor a high intensity flashlight, whistle, personal attack alarm, and safety helmets if required by the site.

b. The Contractor shall further provide the necessary number of under vehicle mirrors (with light facilities) to meet the requirement to search vehicles.

c. The Contractor shall further provide guards and supervisors, whilst on duty, with a reliable man-portable personal radio, and its accompanying controlling base station, to a scale to be agreed between the Contractor and the DO.

d. The DO will undertake to provide for the use by the Contractor's staff such specialist search and communications equipment as may be deemed necessary for their contracted tasks.

e. The Contractor shall ensure that no unauthorised personal items of clothing or equipment are worn/carried by his employees while employed under the terms of the contract.

f. The contractor shall provide adequate high visibility clothing for personnel engaged on access control and on traffic control duties.

Code of conduct

13. Contract guarding personnel will be contractually expected to abide by the MOD's "Code of Conduct for Guards" (see Annex F). This Code amplifies the basic code of conduct contained in BS 7499. The DO is to report any contravention of the Code as a breach of contract. Any member of the CGF who is in breach of the MOD's Code of Conduct may be refused access (by the DO) to the MOD property being guarded under the terms of the contract.

Management and supervision by contractor

14. The Contractor's manager is to liase with the DO, and act as the "point of contact" to supervise and monitor the performance of the guards. The manager should personally visit the site at least once every 10 days and not always by day if 24-hour cover is being provided. In addition, the Company should be required to provide a separate inspectorate capability from their local area office which will visit each site at random intervals at least once per 24 hours for normal periods and once

per shift out of normal working hours including at weekends and public holidays (inspection at more frequent intervals can be arranged under the terms of the contract if so required by the DO).

15. Contractor's guards are to be supervised in the first instance by management staff specially chosen and named by the Contractor. Their selection and appointment is to be based on appropriate expertise, training and experience. There are both "management" and "security" considerations in deciding whether a supervisor should be employed on a guarding post or separately; the supervisor will normally be employed separately from a guarding task unless the alternative is acceptable to the Security Authority. For every 4/5 guard posts manned at one time, the Contractor should employ a Supervisor grade.

16. During silent hours duties, frequent communication between site and area control either by telephone or radio is essential; the frequency may be varied according to the importance of that which is being protected but once per hour is normal with irregular "reverse" calls being made by Control to ensure that all is well; any missed calls from the site should be investigated immediately by the Company.

Supervision by the DO

17. The guard force on duty is to be wholly responsible to the requirements of the DO in execution of their agreed tasks. Guards on duty are to be visited, not less than once every 24 hours by the DO's staff or representative, this may be in conjunction with the Contractor's Inspectorate.

18. The guard force is to be tested in the execution of their agreed tasks not less than once a year by the DO (who should consult the TLB Principal Security Adviser (PSyA) over details of the execution of the test and assistance from the local Security Unit if required). The Contractor's Inspectorate may attend such exercises as observers. The DO is to render to the Contractor a report on each occasion of a test and within 30 days of that test on the effectiveness and performance of the guard force; for their part, the Contractor shall respond to that report within 30 days of receiving the report. No on-site training or exercises are to take place without the permission of the DO.

19. In an emergency the DO will have the right to order the Contractor's staff on duty to perform such reasonable tasks as may be necessary for the security of the site. Any such emergency task must be reported to the Contractor, the Commercial

Staff (CS) and the TLB PSyA as soon as reasonably possible. See Annex G, Paragraphs 3 and 4.

Industrial action

20. In the event of industrial action by any of the guards on the establishment premises, the DO is not to interfere but is to inform the Contractor and in the first instance ask him to provide alternative arrangements. If he is unable or unwilling to

do so the DO is to seek alternative guarding arrangements from the PSyA (if deemed necessary, depending on the scale of the industrial action) as an immediate action. Full details of the industrial action are to be forwarded to the CS.

This page intentionally left blank

APPENDIX 3 TO ANNEX C

GUARD FORCE VETTING

1. **Paragraphs 1 to 6 must be read in conjunction with JSP 440, Volume 2, Chapter 10.** All contract guards employed by the MOD are to have basic check (BC) approval and counter terrorist check (CTC) clearance. Depending on the guard's duties, it may be necessary to conduct a security check (SC); details of these procedures are contained in JSP 440 Volume 2.

2. On award of the Contract, the Contractor is to forward a completed Basic Check Verification Record (BCVR) and MOD Form 1109 in accordance with DEFCON 76 to the HOE for each intended employee at the site under the terms of the Contract.

3. On receipt of the MOD Form 1109 and BCVR, the HOE is to satisfy himself that they contain sufficient information on the prospective guard for the award of the BC clearance. The award of BC clearance is to be recorded by the HOE and the supporting documentation retained on the applicant's file.

4. The HOE is to forward the original MOD Form 1109 to the relevant Vetting Agency for completion of a CTC. A copy of the original MOD Form 1109 is to be retained by the HOE for record purposes. The Vetting Agency is to report the granting of a CTC to the HOE and this clearance is to be recorded.

5. In forwarding the BCVR and MOD Form 1109, the Contractor is to confirm in writing (using the proforma at the end of this Appendix) that they have themselves carried out a background check on the prospective guard covering the previous 3 years, or a lesser period for recent school leavers, consulting former employers as necessary, and have no reason to doubt the reliability of the guard or supervisor. In this context it should be noted that the security companies do not have access to the Police National Computer, nor are they exempt from the Rehabilitation of Offenders Act.

6. The Contractor should be required to give not less than 3 month's notice to the DO, should the Contractor wish to assign Guards or Supervisors who are, or have been, employed on duties concerned with a foreign embassy or a company abroad. The DO is to notify the appropriate TLB Principal Security Adviser (PSyA) and provide as much detail as possible.

PROSPECTIVE EMPLOYEE - STATUS REPORT

To: (Designated Officer)		
From: (Company) (include full postal address and telephone and fax numbers)		
	Telephone:	
	Fax:	
Date:		
Contract number:		

Details of Prospective Employee

Surname	
Forenames (in full)	
Date and Place of Birth	
Age of guard	
Role (either Guard/Supervisor/Manager)	
National Insurance Number	

It is confirmed that:-

a. Full background enquiries have been completed to BSIA or equivalent standards covering the last _____ years without adverse result.

b. There is no reason to doubt the identity of the subject.

c. He/she has successfully completed the MOD Unarmed Guard Initial Training Course under the auspices of the Security Industry Training Organisation Ltd.

Certificate Number		Date of Issue	

d. He/she is medically fit for employment as a guard/supervisor.

e. Before assuming employment the guard/supervisor will be provided with full uniform.

6. It is understood that the above-named cannot be employed on the above assignment until approval is given by the Designated Officer or his representative.

7. BCVR & MOD Form 1109 are attached and details are correct to the best of my knowledge.

Signed for Contractor			Name in Blocks		
Date		Position in Company		Telephone No	

8. Approval is granted for the above named to work under the terms of the above Contract:

Signed for Head of Establishment			Name in Blocks		
Date		Appointment		Telephone No	

NOTE: 1 copy to be retained by the Designated Officer and 1 copy to be returned to the Contractor.

This page intentionally left blank.

ANNEX D

TRAINING OF COMMERCIAL GUARDS

Training Standards

1. All contract guards and on-site supervisors, including those who form the mandated reserve pool and normally work elsewhere, are to have successfully completed the MOD Unarmed Guard Training Course (MUGTC) prior to commencing their duties.

2. The MUGTC consists of:

   a. The MOD Unarmed Guard Initial Training Course (MUGITC) (5 days).

   b. The MOD Unarmed Guard Induction Training Course (MUGInTC) (1 day).

MUGITC

3. The course documentation is held by the Security Industry Training Organisation Ltd (SITO), the National Training Organisation for the Secure Environment. A summary of the course training objectives is at Appendix 1. The MUGTC may only be taught by instructors who have successfully completed the SITO "Train the Trainers Course Parts I and II" and the "SITO/MOD Train the Trainers Part III Assessment Module". All guards and on-site supervisors must successfully complete the MUGITC before they commence work.

MUGInTC

4. The course documentation is held by SITO. All guards and on-site supervisors must successfully complete the MUGInTC during their first 2 days on-site, as part of their induction process. Guards nominated for the reserve pool may complete the MUGInTC up to 12 months prior to employment. If not employed on-site over a 12 month period, they must retake the course to remain eligible for employment.

Continuation Training

5. There is a requirement for a minimum of 13 hours of on-site continuation training to be completed over a two-year cycle after 1year in-post, for each guard and on-site supervisor. The training is mandatory and Companies must provide sufficient manpower to accommodate the requirement. Companies are to:

a. Record details of training in individuals' Personal Development Log Books (PDLB) which are issued by SITO. Logs books are to be made available for inspection by the HOE/DO as required.

b. Send a consolidated return of continuation training carried out to SITO Operations Department every three months. The return is to show the following details:

(1) Company name.

(2) MOD Site at which contract is being conducted.

(3) A separate section for each Training Subject carried out showing date of training and details of individuals who received the training.

(4) Confirmation that training has been recorded in individual PDLBs.

Supervision of Training Standards

6. SITO will maintain a database, on behalf of MOD, of all instructors who are qualified to teach the MUGTC.

7. SITO will maintain a database, on behalf of MOD, of all guards and on-site supervisors who have sat and passed the MUGTC. A list of all personnel so qualified will be provided to the HOE by the contractor prior to the start of the contract. Untrained personnel may not be used for guarding except in extremis when no alternative is available. Prior authorisation in this instance is to be obtained from the HOE. If this happens on a frequent basis, the PSyA is to be informed by the HOE and consideration is to be given to terminating the contract. On passing the MUGTC personnel will receive a PDLB from SITO in which Initial, Induction and Continuation Training and NVQ achievements will be recorded. This book must be available at all times for inspection by SITO/MOD representatives.

8. All companies must allow the SITO auditing team and/or MOD Inspection teams access to their training courses, training records and to inspect their employees PDLBs. TLB PSyAs may initiate such an inspection at any time. HOEs who have any doubts about the training standards of any guards at their establishments should request an inspection by the appropriate PSyA. A full audit report is to be submitted to the appropriate PSyA and D Def Sy.

9. HOEs may contact SITO direct to consult the databases of either Qualified Trainers or Trained Guards. This can be achieved by contacting the Operations Department either by e-mail (address: info@sito.co.uk) or by facsimile (fax number: (01905) 724949). Telephone calls will not be accepted initially until the contact has been authenticated by one of the approved methods.

10. Company Training Staff wishing to obtain information from the database must apply in writing to SITO Operations Dept quoting their individual SITO Trainer's Number.

Access to the MUGTC

11. Contract guarding companies requiring access to the MUGTC must follow the procedures below:

a. Provide SITO with a list of instructors who are to teach the course (by fax or e-mail – see Paragraph 9 above) and confirm that all have successfully completed the SITO "Train the Trainers Course Parts I and II" and the "SITO/MOD Train the Trainers Part III Assessment Module". SITO will verify the list against their records.

b. Purchase from SITO the approved training materials. These can be bought as individual packages or under licence for multiple in-house reproduction. Training may only be delivered using this material.

c. Conduct the MUGITC training and examinations.

d. Submit examination results to SITO for verification and certification. At this stage SITO will record all candidates' details onto the maintained MOD database.

e. Issue guards and on-site supervisors who have successfully completed the MUGITC with their PDLB after first recording the result of the MUGITC.

f. Conduct the MUGInTC training and examinations.

g. Submit examination results to SITO for verification and certification.

h. Record the results in candidates' PDLB.

Validation of Training

12. Validation of the training course will be carried out by D Def Sy periodically.

NVQ/SVQ

13. The company must have a training programme in place which will ensure that within 9 months of the start of the MOD contract at least 30% of its guards allocated to the contract will possess:

A. a National Vocational Qualification (NVQ)

or

B. Scottish Vocational Qualification (SVQ) in Security, Safety & Loss Prevention to Level 2.

The company must also ensure that it can maintain that level of NVQ/SVQ involvement for the duration of the contract.

APPENDIX 1
TO ANNEX D

THE MOD UNARMED GUARD INITIAL TRAINING COURSE

1. The MOD Unarmed Guarding Initial Training Course Training Objectives are:

a. Understanding the threat.

b. Understanding the role of an unarmed guard.

c. Understanding the purpose of a security post.

d. Execute access control duties.

e. Execute procedures for dealing with visitors.

f. Handle persons under the influence of alcohol.

g. Execute traffic control duties.

h. Handle lost and found property.

j. Write reports and notebook entries.

k. Execute an effective search of vehicles, buildings and people.

l. Communicate using correct telephone and radio procedures.

m. Execute a patrol.

n. Powers of Arrest (Common Law; Statute; Demonstrations).

o. Fire-fighting and Fire Prevention.

p. Implement general emergency procedures.

q. Classified documentation and security containers.

This page intentionally left blank

ANNEX E

STATEMENTS OF REQUIREMENTS

Introduction

1. Once the HOE has reached a decision that commercial guarding would be appropriate for the site, the sequence of events at Annex B is to be followed in full consultation with the PSyA and Commercial Staff (CS). Before tenders can be sought by the CS, the security requirements must be clearly defined by the sponsor establishment in a Statement of Requirements (SoR), also known in some areas as a Statement of Security Requirements (SSR). The SoR should comprise the site specific, mandatory security requirements. These requirements should take the form of stating the output required of the contractor, for example "to deny access to the site by unauthorised persons" rather than to state an input requirement "x number of access control personnel to be employed". In this way, responsibility for denying access rests with the contractor should a breach occur. Factors to be considered in preparing the SoR are set out below. The TLB PSyA must be consulted on the contents of the SoR. The Commercial Staff should also advise during its preparation.

2. The SoR will form the basis of the contract resulting from the tendering exercise. The contractor is only bound to perform the requirements specified in the contract.

Factors to be considered in drawing up a statement of requirements

3. The SoR will vary according to the nature of the site to be guarded and the availability of physical protective security measures. When drafting the SoR, site security must always be borne in mind because copies of the SoR are likely to be circulated to a number of firms, only one of which will eventually be awarded the contract. Existing security measures should only be described on a ‘need-to-know’ basis, and SoR will normally be protectively marked RESTRICTED. The management of companies circulated should be advised to protect all such information accordingly. Establishment contingency plans should not be included in the SoR. Any security sensitive aspects of the proposed contract may be covered verbally during the on-site briefing conducted by the HOE and attended by the PSyA, CS and Contractors who have been invited to tender.

4. However, it is most important that the requirement is described as clearly, comprehensively and unambiguously as security considerations will allow as the SoR provides the template against which the Invitation to Tender (ITT) will be framed and tenders evaluated. In turn the ITT will form the basis of the Contract and thus define the criteria that the Contractor will be required to meet in performance. The HOE must bear in mind that he will have no grounds for future complaint should a requirement not be specified in the Contract. The CS are available to give advice and should be consulted during the drafting stage of the SoR. Once approved by the

PSyA, the HOE is to forward the SoR, together with financial approval from the budget manager, to the CS who will invite competitive tenders based on the SoR.

5. In preparing the SoR, the HOE and PSyA should cast it in terms of defining the task or output required of the Contractor, rather than an input in terms of specifying the number of guard posts required for each task. The latter is a matter for the prospective bidder to consider having been given the task(s) and will be judged by the HOE and PSyA at the technical evaluation phase of the contract process. Note, however, that a minimum-manning ratio of 4 personnel to each 24-hour guarding post is mandated at Paragraph 1814 of this Chapter.

6. One essential part of the Contract is a list of quantifiable and auditable performance indicators to be agreed by the CS, the PSyA, the HOE and the Contractor. This list will form the contractual basis for any evaluation of shortfalls by the Contractor and evidence in support of the Contractor's submission for renewal of contract.

7. The following is presented as an aide memoire in drawing up the SoR:

a. **Command and Control:**

(1) Chain of Command within contract guard force including qualifications of managers and supervisors as appropriate.

(2) Supervisor's responsibilities and the name of his immediate superior within establishments.

(3) Aspects of military command procedures where they affect civilian personnel employed by the contract guard force.

b. **Site or Building Access Control:**

(1) Guard and supervisor requirements - to include powers in exercising access control with regard to arrest/detention/searching of individuals (also adequate meal and break reliefs).

(2) Searching of vehicles and baggage.

(3) Calling for escorts.

(4) Identification and issue of passes.

(5) Responsibility for keys.

(6) Requirement for communications.

(7) Responsibility towards deliveries by tradesmen, etc.

c. **Site Patrols:**

(1) Tasks during and outside working hours.

(2) Composition and frequency of patrols.

(3) Calling for escorts.

(4) Identification of visitors and issue of passes.

(5) Requirement for clock stations or other patrol management systems.

(6) Location of backup and acceptable callout delay time.

d. **Building Checks and Internal Patrols:**

(1) Tasks to include security sweeps, periodic security checks and power supplies.

(2) Frequency of patrols.

(3) Buildings that are excluded.

e. **General Responsibilities:**

(1) Reporting of incidents and to whom reports should be made.

(2) Compliance with establishment orders, including security orders.

(3) Parked vehicles within the perimeter.

(4) Alarm systems.

(5) Maintaining normal records such as an incident book, roster register, lost/found property book, local orders and instructions.

f. **Emergency Procedures.** Outline actions required in the event of**:**

(1) Actual attack.

(2) Intrusion or attempted intrusion.

(3) Discovery of a suspected Improvised Explosive Device (IED).

(4) Bomb threat (direct or by telephone).

(5) Fire.

(6) Mains service failure.

(7) A change in the alert state.[1]

g. **High Profile Visitors:** Additional security requirements.[2]

h. **Communications:**

(1) Inter-communication within the guard force.

(2) Responsibilities toward telephone manning and checks.

(3) Communications off site where appropriate.

j. **Conditions of service:**

(1) Security approval and vetting.

(2) Medical fitness.

(3) Hours of work.

(4) Training standards (The training standards at Annex D are to be adhered to).

(5) Code of conduct.

(6) Performance indicators.

k. **Guard Force Facilities (**The SoR will need to specify who will provide which facilities i.e. either MOD or the Contractor):

(1) Heated guardroom.

[1] See Annex G, Paragraph 3 for the requirement to insert a Security Enhancement Clause in all commercial guarding contracts
[2] Ditto

(2) Furniture.

(3) MOD telephone.

(4) Lavatories and ablutions.

(5) Cooking or messing facilities.

(6) Guard force responsibilities for cleanliness.

(7) Transport if required.

(8) Provision of emergency medical treatment.

l. **Additional/Reserve manpower.**

m. **Health and safety provisions.**

8. The SoR should also reflect the Unit/Establishment additional security requirements for heightened BIKINI Alert States or any other contingency plan which could be activated during the period of the contract and involve increased guarding over and above the norm.

9. The performance requirements to be monitored by the HOE contained in Appendix 3 to Annex C are to be covered in the SoR as a contractual obligation on the employer. Similarly, the vetting requirements contained in Appendix 3 to Annex C are to be included in the SoR.

10. The SoR will form the basis of the contract resulting from the tendering exercise. Only the requirements specified in the Contract will be performed by the Contractor. Accordingly, it is essential that any proposed changes to the SoR which may arise during the evaluation process must be scrutinised and approved by the HOE and the PSyA before the contract is awarded.

This page intentionally left blank.

ANNEX F

CODE OF CONDUCT FOR COMMERCIAL GUARDS EMPLOYED BY MOD

Introduction

1. The principal function of the Guard is to support the maintenance of security at MOD units and establishments where the Guarding Contract applies.

Personal Qualities

2. Commercial Guards employed on MOD Contracts are required to uphold the fundamental values and requirements inherent in the Rule of Law. In doing so, each individual will need to exhibit the following personal qualities:

a. Honesty.

b. Integrity.

c. Impartiality.

d. Common sense.

Code of Conduct

Respect for the Individual

3. Guards are expected to show respect for the dignity of the individual at all times, and every individual must be treated with courtesy and understanding irrespective of their social position, race, colour, gender, rank or creed.

Professional Approach

4. Guards must strive to maintain the highest standards. The manner in which Guards approach their duties will influence the way others measure their efficiency and ultimately the effectiveness of what they do.

Rule of Law

5. The Law (Statute and Common) reflects rules imposed upon the community that are binding.

Exercise of Powers

6. Guards must carefully weigh up all factors; be fair and firm but above all avoid intolerance, over-enthusiasm and being dictatorial. They must show caution when acting upon suspicion and comply with the law concerning citizen's powers of arrest. (The Police and Criminal Evidence Act 1984, Section 24 and Criminal Law Act 1967, Section 3).

Breaches of the Code

7. Guards are to abide by the following code of conduct: committing, or condoning, any one of the following will be regarded as a breach of this code of conduct:

a. Neglecting or, without due and sufficient cause, failing to carry out promptly and diligently a required task within their Job description whilst at work.

b. Leaving a place of work during any period of duty without due permission or sufficient cause, or failing to work to the agreed shift pattern.

c. Knowingly making or signing any false oral or written statement.

d. Destroying, mutilating, altering or erasing any official document or record.

e. Divulging to any other person, who does not need to know, any matter which is protectively marked or is the private business of the MOD or contractors, past or present.

f. Soliciting or receiving any bribe or other consideration from any person.

g. Failing to account for documents, keys, a pass or passes, money, or property received in connection with their duty and/or the MOD's business.

h. Being uncivil to persons encountered in the course of their duty, or abuse their position of authority in connection with the discharge of the MOD's business.

i. Acting in a manner reasonably likely to bring discredit upon the MOD, or to fellow employees.

j. Wearing the uniform provided by the Company incorrectly or using MOD equipment without authority.

k. Carrying out or reporting for duty whilst under the influence of alcohol, controlled drugs, or solvents, or to consume any of these while on duty. Guards are to advise their supervisor if their performance may be affected by drugs prescribed by a medical practitioner.

l. Failing to report forthwith to the Designated Officer through the Commercial Guarding Management any conviction for a criminal or motoring offence (other than a minor motoring offence which does not impact on the effective discharge of official duties).

m. Allowing any access to MOD premises by any unauthorised person or persons.

n. Whilst on duty carrying any unauthorised equipment not issued to him/her as part of their duties, (eg handcuffs and truncheons).

o. Failing to report for duty at the correct time and place unless due notice and reasons have been given to their supervisor.

p. Sleeping whilst on duty.

q. Smoking or carrying any smoking materials including matches and cigarette lighters, in any prohibited place where such activities and materials are banned.

8. Any breach of this Code of Conduct may render the individual to be unacceptable for employment on MOD property; in such a case the Contractor will be notified by the Designated Officer accordingly and will replace the offending individual forthwith.

This page intentionally left blank.

ANNEX G

SECURITY CONSIDERATIONS ON COMMERCIAL ISSUES

Evaluation of Tender Bids

1. Commercial Staff (CS) are responsible for making a recommendation for the award of a contract to the HOE, with input from the TLB Principal Security Adviser (PSyA) in evaluating the technical aspects of the bid.

Notification on Awarding a Contract

2. Once a contract has been let CS are to notify D Def Sy, copy to the PSyA, on the proforma at Annex H. The HOE (through the Project Officer) is to be furnished with a copy of the contract.

Variation of Requirement

General

3. An alteration to the guarding posture may be required due to a change in the overall threat level, reassessment of the security of the location concerned by the relevant security staff, or due to particular security requirements for a specific event (e.g. a VVIP Visit). Thus, all guarding contracts are to contain a Security Enhancement Clause (SEC) to meet the additional requirements of higher Alert States. The contract should state that in the case of a change to the threat level the Designated Officer (DO) has the right to invoke the SEC without prior permission. (See Annex C, Appendix 2, Paragraph 19). The DO should familiarise himself with the contract documents which may have procedures which differ from those detailed below.

Implementation of the SEC in an Emergency

4. As stated above, the DO must have the right to invoke the SEC if a higher Alert State is declared and additional guards are required. Higher Alert States will either be declared on a national basis or on a local basis to meet a specific threat. In either case the higher Alert State will be imposed for a short period, normally not more than 5 days. Another case for invoking the SEC might be the establishment receiving a high profile visit requiring additional guards and the fact of a visit needing to be protected until the latest possible moment. The following procedure for the emergency implementation of the SEC is to be adopted:

a. DO confirms the requirement with the PSyA;

b. The DO calls on the Contractor to provide the additional guards specified in contract;

c. CB is notified by the DO immediately the commencement or cessation of the requirement occurs and the number of personnel/hours involved. A signal or fax to CB is acceptable providing the fax is followed up with a financially endorsed Requisition Form for Contract Action within 14 days so that contract amendment can be processed to enable the Contractor to make a claim for payment.

Permanent Amendment to a Contract

5. Where a permanent change to the SoR is needed an amendment reflecting that change should be made to the Contract. All discussions with regard to an amendment to a contract are to be channelled through the CS. In all such cases contractors must not be instructed to carry out any work until formal contractual authority has been obtained from the CS. Failure to do so may result in non-payment and therefore DOs must clearly understand the rules. The procedure for the DO is as follows:

a. Identify the extra (or decreased) requirement in consultation with the PSyA.

b. Prepare SoR to reflect the change, this should be as detailed as possible.

c. Obtain financial approval for the proposed change, and then forward the financially endorsed requisition to the CS.

d. CS will then negotiate with the Contractor and agree a price for the proposed amendment, and then issue a formal amendment to the contract.

Monitoring and Review of Contracts

6. The HOE is responsible for monitoring the Contractor's execution of the Contract. To achieve this in a quantifiable manner, Performance Indicators, set out in the Contract, are to be audited at stated intervals and a report is to be forwarded to the PSyA, copy to the CS and the Contractor. Less formally, the DO is to observe day-to-day performance by the guard force and maintain an incident log to be used in discussion at the regular meetings with the Contractor and as evidence should the Contract require a formal review.

7. Advice must be sought from the CS on the remedies to be pursued when a Contractor fails to meet contractual obligations. Serious consideration must always be given to the termination of a contract if a contractor repeatedly fails to meet his

obligations. For example, any evidence that the contractor is working his staff on shifts in excess of what is permitted in the contract should be recorded and reported as a breach. The CS will write to the Contractor to ensure that the MOD's contractual rights are safeguarded. Minor problems should be covered in regular monthly contractor/client meetings, but all indications of dissatisfaction (including those dealt with orally at local level) are to be recorded and kept on file. More serious breaches should be notified immediately in writing to the CS, copy to the PSyA. If the report is deemed by the PSyA to be particularly serious, for example the incident calls the functioning of the company, as opposed to individual employees of the company, into question, or is likely to attract media attention, D Def Sy is to be notified. PSyAs are to include details of all serious instances of breach of contract in their annual security report to D Def Sy.

Change in Role

8. If it is likely that the location to be guarded will have a change of occupancy/role which may invalidate the use of commercial guards, the change is to be reflected in the terms for terminating the contract.

MGS Competing with Commercial Guarding Companies

9. Ministers have accepted a HCDC recommendation (HCDC Session 1995-96) that the MGS should be allowed to compete with the commercial sector for manned guarding requirements under the Competing for Quality (CFQ) concept. MGS are allowed to compete against the private sector when:

a. Commercial guarding contracts are due for renewal.

b. When the current provider is the MGS and commercial guarding is being considered.

c. Under a multi-service contract either to provide guarding services as a sub-contractor to short list bidders or to provide support to the local In-House Bid Team.

TUPE

10. When permanent MOD staff are to be transferred under the Transfer of Undertakings (Protection of Employment) Regulations 1981 (TUPE), advice is to be sought from Command Secretariats and Civil Management. The sensitivity of industrial relations, particularly where permanent staff are to be transferred under TUPE, should not be underestimated. Where redundancy may result, Ministers may need to be informed. Command Secretariats and Civil Management will advise. Where MDP and/or MGS may be involved, the relevant HQ should also be consulted. All TUPE transfers of MOD staff are to be managed in accordance with the "Code of Practice for TUPE Transfers in MOD Contracts" which has been agreed

with TUs and Industry. This code of practice is to be used by all parties involved in contracting with MOD and outlines best practice to be followed for the transfer of staff under TUPE from MOD to the private sector, or between contractors.

ANNEX H

RESTRICTED - COMMERCIAL
(When completed)

CONTRACT START/RENEWAL PROFORMA

Complete white boxes as appropriate

Contractor Name:					
Address:					
Contract Reference:				Cost per year:	£
Contract start date:		Contract end date:		Total cost:	£
Unit/establishment being guarded					
Name of Designated Officer (DO)			Telephone no:		
Commercial Staff:			Telephone no:		
TLB of Establishment being guarded:					

Type of guarding (Tick the appropriate box if the activity is included in the contract)

Area	Perimeter	Access Control	With Dogs	Without Dogs

Composition of Guard Force (Tick box if Commercial Guard Force is integrated with any of the following)

MDP	MGS	MPGS	Other CGF	Service Personnel	Service Police

Shift pattern

No of guards per shift:		No of shifts per day:	
No of hours per guard per week:		Total complement of guards to fulfil the contract, including a reserve to cover sickness and leave etc:	

Remarks:/Any other relevant information:

(when completed)
RESTRICTED – COMMERCIAL

This page intentionally left blank.

GLOSSARY OF TERMS

The definitions given in this glossary are intended for use specifically within the terms of this manual for dealing with Defence security matters. Some terms shown below are more precise or particular than when used for general purposes and defined elsewhere (e.g. in Joint Warfare Publication 0-01.1 - United Kingdom Glossary of Joint and Multinational Terms and Definitions).

Access control — Control over the flow of information.

The prevention of unauthorized access.

Additional markings — See special markings.

Agent — A person who is recruited, trained, controlled and employed to obtain and report information for intelligence purposes.

Ammunition — The term includes all forms of ammunition, explosives, detonators, pyrotechnics and anti-riot agents but excludes inert items and substances.

Arms — All man-portable weapons, including:

Weapons removed from armoured fighting vehicles or helicopters.

Infantry mortars.

Man-portable anti-tank weapons, e.g., MILAN.

Machine guns, sub-machine guns, pistols, full bore rifles and small bore weapons.

Certain drill purpose (DP) weapons.

Privately owned weapons (including shotguns) which have been accepted for establishment storage.

Flare and pyrotechnic pistols.

Asset — Anything of value, either tangible or intangible, that is owned or used by an organisation or business.

Asset value — The impact of the compromise (breach of confidentiality, breach or loss of integrity or loss of availability) of an

asset.

ATOMAL — A NATO marking applied to documents containing information provided by the government of the United States to other NATO member nations under the agreement between the parties to the North Atlantic Treaty for co-operation regarding atomic information 1964.

ATOMIC — A UK national marking applied to information protectively marked CONFIDENTIAL or above which reveals either directly or indirectly information about:

- The design and fabrication of nuclear warheads.
- Certain features of the design and fabrication of inertial confinement fusion, including laser fusion systems.
- The costs and production rate or stockpile of nuclear warheads.
- Certain features concerning the production, handling and stockpile of fissile, fissionable and special materials used in nuclear warhead.
- Certain features of the design of naval nuclear propulsion plants.
- The production rate of naval nuclear propulsion plants.
- Certain other categories of nuclear information as advised by the Atomic Energy Authority.

ATSy — The application of air transport security measures.

Audit — An independent review by the DSSO of the systems and structures in place to support the TLB security risk management processes.

Automated access control system — Entry control system based on technical means.

Availability — Continuous or timely access to information, systems or physical assets by authorized users.

Barrier fence — A fence used to delineate an area where access may need to be controlled in certain circumstances, e.g., in the event

	to be controlled in certain circumstances, e.g., in the event of a heightened threat. Such a fence is of limited security value but it deters casual intruders and channels pedestrian and vehicular access.
Baseline measures	Measures or a combination of measures which will provide an acceptable minimum level of protection at each level of the protective marking system.
Baseline objectives	The minimum level of security to be reached by a combination of baseline measures at each level of the protective marking system.
Basic Check (BC)	This is NOT a security check but merely a means to provide a degree of assurance of identity, nationality and integrity. MOD Employees with basic check alone are only allowed access to government assets marked RESTRICTED and CONFIDENTIAL under normal supervision.
BIKINI	The unclassified codeword used as the name of the alert system in Great Britain and elsewhere to give warning of possible terrorist activities and the counter measures to be taken.
Bolt box	A container approved by security staffs as sufficiently secure for the storage of weapon bolts/working parts. Boxes must be secured by a security pattern mortice lock or a security approved robust padlock and robust hasp and staple. They must be bolted to the floor or wall. (A similar box, bolted to the structure of a building, may be used for the storage of .22 ammunition when approved by the security staffs).
Bound books	Publications permanently and securely bound from which the pages cannot be detached except by force, cutting or tearing or by deliberate destruction of the controlling binding.
Boundary fence	A fence used to delineate an area.
Branch Security Officer (BSO)	An officer appointed by the senior staff officer of a branch of a headquarters to be responsible for the security arrangements within that branch. Attendance on an establishment security officers course is mandatory.

Breach of security — Anything which prejudices security or contravenes security regulations.

Briefcase (approved) — An approved briefcase is a robust, commercial type briefcase which has nothing in its appearance to connect it to the Armed Forces or the Ministry of Defence. It must have two good locks and will not burst open if dropped.

Categories of establishments — To assist in deciding priorities for the allotment of security resources (e.g., for security surveys and inspections and guarding) establishments are placed into categories.

Categories of loss, compromise and finds — Cases of loss, compromise or finds of protectively marked documents or equipment are categorized as follows:

Category 1 - All TOP SECRET, IDO, ATOMIC and Codeword material. Also COMSEC material (which means all documents, aids, devices or equipment, including CRYPTO material, associated with the securing or authentication of telecommunications).

Category 2 - SECRET material.

Category 3 - CONFIDENTIAL and below.

Caveats — See Special markings.

Civil security — Civil security is the application of measures to the civil population to control its activities. Such measures are distinct from those used for protective security in that they affect the population in its way of living, e.g., control of aliens by entry visa, labour permits and registration are civil controls, whereas control of access to MOD establishments by passes and permits is a protective security measure. Civil security is normally applied through the civil administration. Measures include control of:

Movement (by curfew, control at ports and airports; control of immigration/aliens).

Identity (by the issue of identity documents and ration documents).

Assembly (by the restriction of meetings and

	assemblies). Communication (by censorship). Publication (by censorship, licensing and restrictions of newsprint).
Close protection duties	The provision of an armed bodyguard to protect a nominated individual from harm.
Codeword	A single word used to provide security cover for reference to a particular protectively marked matter. Codewords are issued to Commands by the Ministry of Defence (DCMC).
Commander	Includes commanders of field force and static formations, garrisons, stations and installations.
Commands	A collective reference to commands and forces under the direct control of the Ministry of Defence.
Communications security	The protection resulting from the measures taken to deny unauthorized persons information which might be derived from the possession and study of protectively marked communications, including telephone conversations, radio, telegraph, fax and data transmissions.
Compromise	Compromise encompasses the full range of means, both deliberate and accidental, by which damage could be caused to Government assets. This includes disclosure, loss, theft, destruction, tampering or accidental damage.
Confidentiality	The prevention of the unauthorized (including accidental) disclosure of information.
Control officer	An officer appointed by a head of establishment to be personally responsible for the safe custody of and accounting for all documents protectively marked TOP SECRET (i.e., TOP SECRET control officer (TSCO)) and/or documents which require special handling (e.g. ATOMIC control officer (ACO)).
COSMIC	A NATO marking applied to NATO documents protectively marked TOP SECRET (i.e., COSMIC TOP SECRET).
Counter intelligence	The NATO definition is: Those activities which are concerned with identifying and counteracting the threat to

	security posed by foreign, including hostile, intelligence services or organizations or by individuals engaged in espionage, sabotage, subversion or terrorism. See also security intelligence.
CRYPTO	A marking applied to protectively marked operational cryptographic keying material. Items so marked are subject to specific controls governing access, distribution, storage, accounting, disposal and destruction.
Cryptographic Custodian	An officer responsible for the custody, handling, safeguarding and distribution of cryptographic material.
Cryptographic keying material	Material used for the settings of encryption devices for cryptographic machines; the settings are changed at predetermined intervals.
Cryptographic material	All documents, devices and equipment which contain information essential to the encryption or decryption of communications.
Cryptographic security	The defence against crypto-analysis which results from the protection given to classified traffic by the use of cryptographic equipment, ciphers and codes.
CRYPTO-SECURITY	A marking applied to documents containing cryptographic information, less keying material (which is marked CRYPTO), the knowledge of which needs to be restricted to individuals authorized to receive it.
Declassification	The correctly authorized removal of any protective marking (including RESTRICTED) from information, documents, equipment or material in order to make them unclassified. Declassification does not of itself authorize release to press or public.
Descriptors	See special markings.
Destruction	In this manual destruction means destroying protected material by the methods approved both for the particular protective marking of the information concerned and for the medium on which it is recorded.
Developed Vetting(DV)	The clearance required for posts involving long-term, frequent and uncontrolled access to assets marked TOP SECRET.

Disclosure Disclosure of information means its communication by one person to another whether intentionally or otherwise. It is said to be authorized when it is passed necessarily in the course of official duty.

Document Any form of recorded information constitutes a document. Apart from printed, typewritten or reproduced papers, the items listed below and others of similar types are treated as documents:

Files, branch folders, manuscripts, notebooks (including shorthand notebooks), and drafts.

Maps, charts and graphs.

Vufoils.

Imagery records, photographs, negative, film slides and films.

Stencils, matrices, carries, masters, and litho plates.

Plain language and machine-readable paper.

Recording tape and punched cards.

Removable IT magnetic storage media of all types.

Paper tape and punched cards.

Visual display unit (VDU) displays.

Microfilm material.

Typewriter ribbons and carbon papers.

Downgrading The correctly authorized replacement of any protective marking from a higher to a lower one. This may normally only be authorized by the originator.

Espionage The acquisition or attempted acquisition of information covertly or illegally to assist a foreign power or to further a subversive political aim.

Establishment Unless otherwise qualified, the term "Establishment" is used throughout this manual to embrace any MOD organization formed on a separate establishment (organisational structure), including formation

	headquarters, units, branches, establishments, air fields, vessels, depots and installations. The term also includes all civilian organizations for which the MOD has a security responsibility.
Establishment Security Officer (ESyO)	ESyO is the generic term for Base Security Officer (BSO) or Unit Security Officer (USO) in the Royal Navy, Unit Security Officer (USO) or Branch Security Officer (BSO) in the Army, Station Security Officer (SSyO) in the Royal Air Force and the appointed chief specialist security officer employed in MOD Agencies or industry.
FOCAL	A Western European Union (WEU) marking applied to WEU documents with the protective marking TOP SECRET (i.e. FOCAL TOP SECRET).
Global security environment (GSE)	The GSE is the general security environment in which the computer system is located. It covers everything outside the control of the systems manager (SM), which may have involved a systems security (e.g. site access control) (see also security domains).
GOCO	A Government Owned - Contractor Operated Venture.
Head of Establishment(HOE)	The term "head of establishment" is used to denote all Service commanders or Civil Service equivalents of any MOD organisation formed on a separate establishment (organisational structure), including formation headquarters, units, establishments, airfields, vessels, depots and installations or civilian organisations for which MOD has a security responsibility. The term includes Chief Executives of Defence Agencies and Chief Executives of GOCO organisations formed on a separate establishment or organisational structure.
Higher Threat Personnel (HTP)	A small number of individuals who have been assessed as at a higher threat of terrorist attack than the majority of Service personnel and for whom certain essential additional precautions for protection are authorized.
Identity card	A document issued for the purpose of establishing the identity of the holder. It is not a pass or a permit.
Information Technology (IT) Security	Measures to ensure the confidentiality, availability, and integrity of information in IT systems.

Integrity	The maintenance of information, systems of all kinds and physical assets in their complete and proper form.
International Defence Organization (IDO)	The words NATO and WEU (COSMIC and FOCAL when NATO and WEU TOP SECRET documents, respectively, are involved) are special markings which, when applied to a document, signify that the document is authorized for circulation on a need to know basis within the IDOs of the North Atlantic Treaty Organization or the Western European Union, respectively, and subject to certain security procedures and regulations of these organizations.
Intruder Detection System (IDS)	Electronic devices used to provide continuous surveillance of an area to detect attempted or actual entry of an intruder and to alert the guard. See also PIDS.
IVCO	International Visits Control Office.
National caveats	See special markings.
National caveats	See special markings.
Need to hold	The principle that protectively marked documents or material are to be held only by those individuals who are authorized and have a need for immediate access to them for the efficient discharge of their official duties, and in those Establishments/areas where there are appropriate arrangements to protect them.
Need to know	The principal that access to protectively marked information is to be restricted solely to those individuals who are authorized to have it and need to know the information to carry out their official duties efficiently.
Nickname	A nickname is made up of two words selected by the originator and used for convenience for reference to any matter where security protection is not required.
Non-List X Company	A firm which is contracted by the MOD but is not authorised to hold protectively marked material above RESTRICTED on its premises. (see also List X Company)
Official information	Information, whether protectively marked or unclassified, in any form, both oral and recorded, which is concerned with the business of the Government or Service activities.

On-line system	A system which performs directly under the control of the central processor, while the user remains in communication with the computer.
Page by page check	A detailed check of individual pages of a publication against an integral list of effective pages (LEP) or in the absence of an LEP, the Table of Contents.
Pass	An approved document which authorizes the holder to pass through a security control.
Perimeter intruder detection systems (PIDS)	Technical measures which may be used to enhance the level of security offered by a perimeter fence.
Permit	An approved document which authorizes the holder to perform a specified act or acts.
Personnel security	That part of protective security concerned with all measures related to personnel designed to counter the threat posed by foreign intelligence organizations or subversive groups or individuals. Procedures include vetting designed to ensure that only persons whose reliability and trustworthiness are not open to doubt have access to classified information.
Personnel Vetting Records Officer (PVRO)	An officer appointed by a head of establishment to keep the records of establishment posts which require security clearance, and of the vetting status of the individuals filling these posts.
Physical security	That part of protective security concerned with physical measures (e.g. fences, buildings, intruder detection systems (IDS), containers and locks) designed to safeguard personnel and material from espionage, sabotage, subversion, terrorist attack, and theft.
Protected compartment	Any compartment containing material protectively marked CONFIDENTIAL and above which depends upon the compartment door for protection, (i.e. the material cannot be locked in a security container).
Protected document	Any medium on which classified information is recorded in either visible or electronic form. See also Protective marking.

Protected Document Register (PDR)	A register (MOD Form 102) kept by an establishment to record the receipt, production, disposal, regrading, declassification, destruction and dispatch of every document classified with a protective marking of SECRET and above, or bearing special markings requiring separate registration e.g., ATOMIC.
Protected equipment register	A register (MOD Form 102 suitably amended) kept by an establishment to record the receipt, disposal, regrading, declassification, destruction, and dispatch of all protected equipment and detachable protected components.
Protected information	Information in any form, both oral and recorded, which is to be safeguarded in the interests of national or international security and which has been classified with a protective marking. See also Protective marking.
Protected material register	See protected equipment register.
Protective marking	A grading given to information or material to show the degree of damage that could result from its unauthorized disclosure and the standard of protection to be given to it. (It should be noted that International Defence Organisations and member nations as well as members of the Commonwealth use protective markings, known as classifications, except RESTRICTED in certain cases, with similar, but less all embracing, meanings.) See also Protected document and Protected information.
Protective marking system	A method of assigning asset values to things to indicate the level of security or protection required. Assets may be marked physically (e.g. with headers and footers on pages of print) or, for risk management purposes, may be "treated as if" they carried a marking.
Protective security	The organized system of defensive security measures (physical security measures and personnel security measures) designed to protect information, material, personnel activities and installations.
Protective security check	A check carried out by, or on the orders of, a head of establishment to ensure that a specific security measure within his establishment is adequate and correctly applied.

Protective security inspection	A routine security inspection carried out for a specific purpose by a security unit to examine, report and make recommendations upon any aspect of the state of security of an establishment. It is additional to a security survey.
Protective security review	An examination carried out by, or on the orders of, a head of establishment of the overall security arrangements within his establishment. The purpose is to maintain the establishment system of protective security.
Protective security survey	A detailed pre-planned periodic security examination carried out by a security unit to examine, report and make recommendations upon the state of security of an establishment. The purpose of survey is to give commanders a clear idea of the state of security in their formations and to provide HOE with assistance and advice in the application of security measures to remedy any identified weaknesses.
Protectively marked assets	Information, material or equipment protectively marked RESTRICTED or above.
Radiation security	The elimination or containment of unintended intelligence-bearing emanations from cryptographic, communications and other electronic equipment (see TEMPEST).
Regrading	Changing the protective marking of items by correctly authorized upgrading, downgrading or declassification.
Risk	The product of threat and vulnerability (normally the lower of the two), that is the probability or likelihood of an attack succeeding; or of sustaining damage as a result of compromise.
Risk management	Reducing to an acceptable level the risk of a successful attack or damage from a compromise occurring; and/or reducing the damage which could be caused. This can be achieved in a number of ways, for example by transferring a part of the risk by insurance or by moving the assets to another site or by protective security. An acceptable risk is when the risk manager is prepared to accept the remaining risk. Risk management is a dynamic process and needs to be kept under review.

Sabotage	An act, falling short of a military operation, or an omission, intended to cause physical damage in order to assist a hostile foreign power, or to further a wider subversive political aim.
Secure ammunition store	See secure armoury.
Secure area	Any part of an establishments location to which access is controlled.
Secure armoury (and secure ammunition store)	(Note: ammunition should not normally be stored in the same room as arms). An armoury or ammunition store which complies with the minimum structural standards laid down in the appropriate SAFE/SSG specification, and is either: a. Visited by a guard or patrol at intervals of not more than one hour when not occupied, or b. Fitted with an approved intruder detection system (IDS).
Secure room	See strong room.
Security	The condition achieved when designated information, material, personnel, activities and installations are protected against espionage, sabotage, subversion and terrorism, as well as against loss or unauthorized disclosure. The term is also applied to the measures necessary to achieve this condition and to the organizations responsible for these measures.
Security area	Any part of an establishment to which access is controlled.
Security Check (SC)	The level of clearance required for posts involving long-term, frequent and uncontrolled access to assets marked SECRET and those which afford occasional and controlled access to assets marked TOP SECRET.
Security colour code	Covers for documents are coloured as follows: TOP SECRET – Red SECRET – Pink CONFIDENTIAL – Green

RESTRICTED – Buff

UNCLASSIFIED - Any colour other than Red, Pink or Green

Security container An item of security equipment approved by the Security Equipment Assessment Panel and supplied by DOE(SSG/SFE) for the storage or carriage of protected material. The container are classified according to the level of security they offer; Class 4 being the highest and Class 1 the lowest.

Security education The instruction given to all Service personnel and MOD civilian staff to keep them informed of the threat to security and aware of their general responsibilities for countering it.

Security fence A fence constructed to an approved minimum standard to assist control of entry to and from an area to be protected, and to deter and delay intruders.

Security intelligence Intelligence on the identity, capabilities and intentions of hostile organisations or individuals who are or who may be engaged in espionage, sabotage, subversion or terrorism. See also Counter intelligence.

Security investigation A security investigation carried out by a security unit at the direction of the security staff to establish the cause and extent of a breach of security, to recommend remedial action, and to assist commanders to minimize the damage done.

Security key A security key is one which operates a lock fitted to a:

Security container for housing classified material.

Door of a secure building, room or area.

Box, security pouch, security briefcase, etc, used for the transmission or circulation of classified documents.

Door of a room which has been given special protection against technical eavesdropping.

Door of an armoury, ammunition or explosives store.

Security alarm box.

Security lock — A lock which has been tested to establish its resistance to both surreptitious and forcible attack and which has been approved by the Security Equipment Assessment Panel. Security locks are divided into four classes: 1 to 4. Class 4 being the highest and Class 1 the lowest level.

Security pouch — An official pouch made of PVC-coated nylon designed for the transmission of classified documents. It is fitted with a shoulder strap and secured by a locking bar with a Chubb 2 in Ava padlock or Abloy 3041 padlock; supplied by HMSO.

Security training — Specialist instruction in the application of security measures for the incumbents of posts which carry specific security responsibilities.

Security units — Security unit is the generic term given to area security teams in the Royal Navy, Intelligence Corps MI and security units in the Army, Provost & Security Services (P&SS) regions in the Royal Air Force and security personnel in the DLO, DPA and MOD Centre.

Security vetting — The routine process for identifying persons who are suitable for access to information protectively marked SECRET or above. There are two levels of security clearance within the MOD: Security Check (SC) and Developed Vetting (DV); other Government Departments may use a third and lower Basic Check (BC).

Service Personnel — All Royal Navy (including Royal Marines), Army and Royal Airforce personnel serving on a regular or reserve basis.

Special handling procedures — Additional systems of control (i.e., restrictions on handling and distribution) applied to certain types of classified information, documents or material, authorized by the Ministry of Defence or security staffs, in order to limit access to specifically nominated individuals.

Special markings — Markings in the form of a phrase, word or abbreviation applied to documents as warnings, which are additional to but do not modify any security classification allotted to them, and which consist of the following:

Descriptors. Markings which are available, if required, to show the nature of sensitive material, e.g.. MEDICAL, HONOURS, CONTRACTS, STAFF (a comprehensive list is at Annex A to Chapter 1). They also indicate the broad categories of people who may have access.

Restrictive markings. Markings used to limit the handling and circulation of documents to those categories of persons authorized to have access to them in order to enforce the need to know principle, e.g. EXCLUSIVE and CONTROLLED DISTRIBUTION REQUIRED. No copy should be made without permission of the originator.

Additional markings. Markings which indicate the conditions of issue/release, origin or ownership of documents.

National caveats. Caveats used to provide additional protection of certain types of UK protectively marked material.

Station Security Officer (SSyO) RAF term for the Establishment Security Officer.

Strong room Strong rooms and secure rooms are specially constructed rooms which provide a specified degree of security protection, according to their structural detail laid down in the appropriate SAFE/SSG specification (which are held by DE), for the storage of classified material. Strong rooms provide a higher degree of protection than secure rooms.

Structurally approved armoury An Army term for an armoury which complies with the minimum structural standards laid down in the appropriate SAFE/SSG specification (which are held by DE), but is not fitted with an approved intruder detection system (IDS), nor visited hourly, nor permanently occupied.

Subversion Activities which threaten the safety or well being of the State and are intended to undermine or overthrow parliamentary democracy by political, industrial or violent means.

Surveillance The systematic observation of aerospace, surface of subsurface areas, places, persons or things by visual, aural,

	electronic, photographic or other means.
Talent spotting	Activity by foreign intelligence services (FIS) and subversive organizations aimed at identifying individuals who are potentially suitable for subversion or coercion to assist hostile activities.
Target	A country, area, installation, agency or person against which espionage, subversion, sabotage, or terrorism is directed.
Telephone privacy equipment (scrambler equipment)	A device fitted to a telephone which provides a degree of privacy against casual overhearing. It does not provide security protection.
TEMPEST	The unintentional radiation or conduction of compromising emanations from communications and information processing equipment.
Terminal	A peripheral device which provides a means of access to a computer system at which data may be input to or output from the system, or at which an individual may control the processing of data.
Terrorism	The use of violence or intimidation in the furtherance of a political aim.
TESSERAL	The unclassified codeword issued as a warning against a possible terrorist SAM attack in the UK.
Threat	The probability or likelihood of an attack or undesirable event (including environmental hazards and natural disasters) taking place. Threat includes such factors as capability, resources and intention and probabilities (e.g. of unplanned, external events occurring).
Threat types	These cover surreptitious attack, e.g. from espionage and leakage, theft, e.g. from burglary or dishonest staff, damage, e.g. from vandalism, hostile members of the public, pressure groups or natural disasters and so on. The threat from terrorism is considered separately and appropriate steps are incorporated into the universal baseline measures.
Transmission security	Defence against traffic analysis, that is, against everything that an intercept organisation can do to derive intelligence

	from a study of traffic short of breaking ciphers. Such measures include use of correct signal procedures, proper message classification and communications discipline.
UNCLASSIFIED	The marking or description given to information which is not protectively marked.
Universal baseline measures	Measures which apply to all assets at all levels of the protective marking system.
Upgrading	The correctly authorized alteration of a protective marking from a lower to a higher one.
Vulnerability	A feature or characteristic of an asset which renders it susceptible to compromise, damage, misuse or unreliability. e.g. a VDU which emits radiation, windows which could shatter scattering lethal splinters of glass in an explosion, or something which makes an asset particularly susceptible to damage in the event of a disaster occurring, e.g. basement accommodation in an area liable to flooding.
Vulnerable Point (VP)	Any point vulnerable to sabotage in or connected with a key point where destruction or serious damage would result in unacceptable interruption of the key points' services or loss of products.

LIST OF ABBREVIATIONS

The abbreviations listed below are intended for use specifically within the terms of this manual for dealing with Defence security matters.

AACS	Automated access control system
ACO	ATOMIC control officer
ACPO	Association of Chief Police Officers
ACTO	Attractive to criminal and terrorist organisations
ADAS	Automated document accounting system
ATSy	Air Transport Security Officer
BC	Basic Check
BID	British Inter Departmental Equipment
BSO	Branch Security Officer
BSSO(G)	British Services Security Organization (Germany)
BSyO	Branch Security Officer (RAF)
BTR	British TEMPEST Regulation
CB(Sy)	MOD Central Budget (Security)
CCRIO	Central Criminal Records and Intelligence Office
CCTA	The Government Centre for Information Systems
CCTV	Closed circuit television
CEAG	Counter Extremist Advisory Group
CESG	Communications Electronics Security Group
CGF	Commercial Guard Force
CI	Counter intelligence
CPF	Civilian Police Forces

COCO	Contractor owned, contractor operated
COMSEC	Communications security
COMSO	Communications Security Officer
CPSyO	Command Provost & Security Officer (RAF)
CSE	Catalogue of Security Equipment
CTC	Counter Terrorist Check
DAC	Defence Audit Committee
D Def Sy	Directorate of Defence Security
D INT CORPS	Director of the Intelligence Corps
DCMC	Defence Crisis Management Centre
DCS	Defence Courier Service
DE	Defence Estates
DGS&S	Director General Security and Safety
DIDC	Defence identity card
DIDCAC WG	Defence identity card and access control working group
DISS	Defence Intelligence and Security School
DMS	Defence Manual of Security (JSP 440)
DP	Drill purpose
DPA	Defence Procurement Agency
DS	Directing Staff
DSO	Departmental Security Officer
DSSO	Defence Security Standards Organisation
DSPC	Defence Security Policy Committee
DSy(Pol)	Director of Security (Policy) - now D Def Sy

DTMA MCC	Defence Transport and Movements Agency, Movements Control Centre
DV	Developed Vetting
DVA	Defence Vetting Agency
EDICTS	Evaluation and development in counter terrorism and sabotage
ERO	Explosive Responsible Officer
ESO	Event Security Officer
ESyO	Establishment security officer
FAX	Facsimile communication equipment
FCO	Foreign and Commonwealth Office
FIS	Foreign intelligence service
FOI	Freedom of Information (Act)
FPS	Focal Point System
GAIs	General Administrative Instructions
GCHQ	Government Communications Headquarters
GOCO	Government owned, contractor operated
HIS	Hostile intelligence service
HMG	Her Majesty's Government
HMSO	Her Majesty's Stationery Office
HOE	Head of Establishment
HTP	High threat personnel
ICO	Incident control officer
IDO	International Defence Organization
IDS	Intruder detection system

IED	Improvised explosive device
ISC	Internal security committee
IT	Information technology
JSP	Joint Service Publication
KP	Key Point
KPC	Key Point Committee
KPSO	Key Point Security Officer (Army)
LCT	London Courier Terminal
LTI	Limited technical inspection
MDP	Ministry of Defence Police
MDT	Mechanical document transfer
MGS	Ministry of Defence Guard Service
Min(AF)	Minister for the Armed Forces
MPSB	Metropolitan Police Special Branch
OGD	Other Government Departments
OTTAL	Overseas Terrorist Threat Assessment List
OSE	Off Site Event
PDR	Protected Document Register (MOD Form 102)
PfP	Partnership for Peace
PIDS	Perimeter intruder detection system
PME	Public Military Event
PSDB	Police Scientific Development Branch
PSI	Protective security inspection
PSS	Protective security survey

PSyA	Principal Security Adviser
RCIED	Remotely controlled improvised explosive device
RMIPC	Release of military information policy committee
ROI	Republic of Ireland
SAFE/SSG	Security Facilities Executive, Special Security Group
SC	Security Check
SCIT(A)	Special Counter Intelligence Team (Army)
SEAP	Security Equipment Assessment Panel
SIGINT	Signal intelligence
SIRS	Security Incident Reporting Scheme
SOP	Standing operating procedure
SSG	Security Services Group
SSOs	Security standing orders
SSR	Statement of security requirement OR Security Structures Review
SSyO	Station Security Officer (RAF)
STP	Services technical publication
STRAPSO	STRAP Security Officer
SVA	Security Vilgilance Area
SyOPs	Security operating procedures
TEMPEST	Radiation security
TF	Trading Fund
TLB	Top Level Budget
TSCO	TOP SECRET control officer

TSI	Technical security inspection
TSU	Technical Security Unit
UARS	Unit Annual Report on Security (Army)
UNIRAS	Unified Incident Reporting and Alert Scheme
USO	Unit Security Officer (Army)
USR	Unit security register
USyO	Unit Security Officer (RAF)
VDU	Visual display unit
VP	Vulnerable Point
XPM	Expanded metal

A

D

This page intentionally left blank.

VOLUME 2
Issue 2

PERSONNEL SECURITY

MINISTRY OF DEFENCE
October 2001

This page intentionally left blank.

VOLUME 2

CONTENTS

INTRODUCTION

Purpose and Description

1. The purpose of the Defence Manual of Security (DMS) Volume 2 (the Volume) is to lay down the personnel security regulations and measures which are to be applied throughout the Armed Services, to MOD civil servants, to the staff of MOD agencies and to contractors' employees working for the MOD or for the Services.

2. DMS Volume 2 is derived from the Manual of Protective Security (MPS), issued by the Cabinet Office, which lays down Government security policy and contains further detailed guidance on personnel security, including the vetting regime. MPS is applicable within the MOD, **except** in those few instances where the MOD has elected, as authorised by the Review of Protective Security (RPS), to take a more restrictive line.

3. The four parts of the volume comprise:

a. **Part 1** – covering the fundamentals of personnel security, including the principles of security and the basics of personnel security; details of the vetting system; and guidance on nationality.

b. **Part 2** – setting out the personnel security vetting measures that apply to Service personnel, to MOD civil servants and to the staff of MOD agencies.

Note: A joint or tri-Service establishment is to apply personnel security measures in accordance with an individual's parent Service.

c. **Part 3** – providing guidance on the vetting of contractors' employees including information on the procedures to be applied to contractors' employees working in Service establishments.

d. **Part 4** – covering the application of personnel security measures including the denial, withdrawal, suspension and lapsing of security clearance, the personnel security responsibilities of heads of establishments (HOE), notification of security clearances on transfer, and travel to countries to which special security regulations apply (CSSRA).

4. To assist users to find the information they require, each chapter is preceded by a list of contents. An index is also provided

Application

5. The regulations and measures throughout the volume apply generally to:

a. All Regular and Reserve Forces of the Royal Navy, the Royal Marines, the Army and the Royal Air Force.

b. Civil servants working in Service units or in MOD establishments including those working on fixed term, casual or short-notice appointments.

c. Agency employees or independent consultants undertaking work in Service units or in MOD establishments.

d. The staff of Defence Agencies and of Government owned contractor-operated (GOCO) sites.

e. Persons serving with the Combined Cadet Force (CCF), the Sea Cadet Corps (SCC), the Army Cadet Force (ACF) and the Air Training Corps (ATC).

f. Contractors' employees working in Service and MOD establishments.

g. Locally engaged civilians (LEC) overseas where regulations may be amended as necessary by local rules.

Relationship to other Publications and Instructions

6. The DMS consists of five volumes. This volume is companion to:

Volume 1 - Protective Security

Volume 3 - Information Technology

Volume 4 - Directive for the Security of Nuclear Weapons and Special Nuclear Materials

Volume 5 - STRAP

7. This volume supersedes the policy elements of the following single Service publications and instructions which relate to personnel security:

a. CB 4005: The Manual of Naval Security Volume II – Personnel.

b. AC 60497(2): The Manual of Army Security Volume 2 – Personnel Security.

c. RAF GAI 5009: Security Restrictions on Duty and Travel applicable to RAF Personnel and Civilian Employees of the Air Force Department.

8. It remains incumbent on single Service authorities and TLBs to promulgate enabling instructions to cover the detailed procedures to be followed by their own recruiting, personnel and security staffs.

9. Single service publications and instructions complementary to this volume are:

a. **Royal Navy:**

(1) BR 8587: Naval Leave and Travel Regulations.

(2) DMS Volume 2: RN Supplementary Instructions.

b. **Army:**

(1) Personnel Security Instructions.

(2) The Army Leave Manual.

(3) AGAI, Chapter 8.

(4) LAND Standing Orders.

c. **Royal Air Force:**

(1) AMP's Vetting Directive.

(2) AP3392: The Manual of Personnel Administration.

(3) Air Secretary's Personnel Staff Instructions.

(4) DMS Volume 2: RAF Supplementary Instructions.

Use of Masculine Gender

10. For brevity, the masculine gender has been used throughout the volume, but the instructions it contains apply equally to male and female personnel.

Definitions

11. A full glossary of terms relating to Defence security matters is contained in the DMS Volume 1 "Protective Security". Terms of particular note used in this volume are:

a. **Aftercare.** Everything of actual security concern (with the exception of periodic reviews of security clearances) or of potential security concern that affects an individual who has been either security cleared or, in the case of non vetted personnel merely BC-approved, is known as *aftercare*.

b. **CPMA.** A civilian personnel management authority with delegated recruiting and posting powers.

c. **Head of Establishment (HOE).** All Service commanders or Civil Service equivalents of any MOD organisation formed on a separate establishment (organisational structure), including formation headquarters, units, establishments, airfields, vessels, depots and installations or civilian organisations for which MOD has a security responsibility. The term includes Chief Executives of Defence Agencies and Chief Executives of GOCO organisations formed on a separate establishment (organisational structure).

d. **List X Company.** A firm which is authorised to hold protectively marked material CONFIDENTIAL or above on its premises commensurate with the use of approved security equipment and physical security measures.

e. **Non List X Company.** A firm which is contracted by the MOD but is not authorised to hold protectively marked material above RESTRICTED on its premises.

f. **Protectively Marked Assets.** Information and material so marked or equipment protectively marked RESTRICTED and above.

g. **Service Personnel.** All Royal Navy (including Royal Marines), Army and Royal Air Force personnel serving on a regular or reserve basis.

h. **Principal Security Adviser (PSyA).** Provide corporate security advice to the Management Board of the TLB Holder/Trading Fund. Oversight and direction of security, including personnel security, across the TLB?Trading Fund.

12. "Recruiting Authorities" are:

a. **Royal Navy:** The Director of Naval Recruiting for RN and RM officers and ratings, Naval Medical, Dental and Chaplaincy branches for doctors, dentists and chaplains; BRNC Dartmouth for URNU members; and the appropriate CPMA for civil servants.

b. **Army:** The Director of Recruiting for officers and soldiers; Army Medical, Dental and Chaplaincy departments for doctors, dentists and chaplains; Territorial Army (TA) units for TA officers and soldiers; HQ

Territorial Army and Volunteer Reserve Associations (TAVRAs) for ACF commissions; and the appropriate CPMA for civil servants.

c. **Royal Air Force:** The Director of Recruiting and Selection (RAF) for members of the regular RAF; the Deputy Controller of RAF Reserve Forces for Royal Auxiliary Air Force and Volunteer Reserves; HQ Air Cadets for Volunteer Reserve (Training) officers, Adult Warrant Officers and Civilian Instructors; HQ University Air Squadrons (UAS) for UAS members; and the appropriate CPMA for civil servants.

d. **Civilians:** Appropriate CPMA.

13. "Posting Authorities" are:

a. **Royal Navy and Royal Marines:** The Naval Secretary for Royal Navy and Royal Marine officer appointments; Commodore Naval Drafting for drafting of ratings; HQ Royal Marines (Manning Office) for RM other ranks; and the appropriate CPMA for civil servants.

b. **Army:** The Army Personnel Centre (APC) for officers and soldiers, MOD Chaps (A) for RAChD and DALS for AGC(ALS) officers plus the appropriate CPMA for civil servants.

c. **Royal Air Force:** The RAF Personnel Management Agency for RAF personnel and the appropriate CPMA for civil servants.

d. **Civilians:** Appropriate CPMA.

Personnel Security Staffs and Defence Vetting Agency

14. The designations and particulars are given in Annexes A and B.

Line Management: Principal Security Adviser Relationship

15. The relationship is set out in Annex C.

Suggestions for Amendment

16. All suggestions for additions or alterations to the text of this Volume are to be addressed, through line management or establishment security officers/the chain of command to:

Royal Navy - DNSyICP AD(P)

Army	-	Head of Pers Sy(A)Sec Copy to HQ LAND G2 Phys/Pers Sy
Royal Air Force		HQ PTC Sy 1
MOD	-	D Def Sy-PersSy2

Distribution and Availability of Volume

17. Copies of this complete volume are distributed to establishments, as necessary, for retention as directed by the HOE. Lead Commands will determine the distribution within the Services and other TLBs for its area of responsibility. The Volume is to be available to those whose duties are to operate the procedures. Local orders should draw attention to the availability of the Volume.

ANNEX A

PERSONNEL SECURITY STAFFS

Sponsor CHOtS address	**Address**	**Telephone/Fax**
MOD Headquarters, **DPA, and Trading Funds**	Director of Defence Security	
DDefSy-DD Pers Sec	Room 328 St Giles Court 1-13 St Giles High Street London WC2H 8LD	0207-218-3760 Fax: 0207-218-1165
Royal Navy	DNSy/ICP	02392-726201
DNSYADP	Victory Building HM Naval Base Portsmouth PO1 2LS	 Fax: 02392-727127
Army	Head of Pers Sy(A)Sec	019064-66-2394
Pers Sy(A) Section Head	Imphal Barracks Fulford Road York YO14AS	 Fax: 01904-66-2398
Royal Air Force	GC Prov & Pers Sy(RAF)	01452-712612
Sy1HQPTC	RAF Innsworth Glos GL3 1EZ	Fax: 01452-712612 Ext 5974

DLO	DLO PSyA	01225-467509
DLOHQ-DLO-PSYA	Spur 11 E Block Ensleigh Bath BA1 5AB	Fax: 01225-467299
PJHQ	SO1 J2-PSyA	019238-46145
PJHQ-J2-SO1-PSYA	PJHQ(UK) Sandy Lane Northwood Middx HA6 3JJ	Fax: 019238-46013

ANNEX B

DEFENCE VETTING AGENCY (DVA)

Sponsor: MOD	**Owner: DG S&S**	
CHOtS address	**Address**	**Telephone/Fax**
CE/DVA	**Chief Executive (CE/DVA)** Building 107 Imphal Barracks Fulford Road York YO1 4AU	01904-66-2444 Fax: 01904-66-5820
DVA YORK- HEAD OF PRIMARY CLEARANCE DIVISION	**Head of PC Division** Building 107 Imphal Barracks Fulford Road York YO1 4AS	01904-66-2225 Fax: 01904-66-2645
DVA YORK – HEAD OF DEVELOPED CLEARANCE	**Head of DC Division** Building 107 Imphal Barracks Fulford Road York YO1 4AS	01904-66-5952 Fax: 01904-66-2645

This page intentionally left blank.

ANNEX C

LINE MANAGEMENT: PRINCIPAL SECURITY ADVISER RELATIONSHIP

Formation	Line Management	Principal Security Adviser
Central TLB	2nd PUS	Hd CB(Sy)
DPA	Chief of Defence Procurement (CDP)	DPA PSyA
Defence Agencies	Chief Executives	TLB/Command PSyA
Defence GOCO Establishment	Chief Executives	TLB/Command PSyA
Royal Navy	Commanders in Chief	DNSy/ICP AD NSy(P)
Army	Commander in Chief Land Command	ACOS Ops/Int/Sy/HQ LAND Head of Pers Sy(A)Sec)
Royal Air Force	Commander in Chief	AO Sy&PM(RAF) (GC Prov&Pers Sy (RAF)HQ PTC)
PJHQ	CJO	ACOS J2 (SO3/J2X)
DLO	CDL	DLO - PSyA

This page intentionally left blank.

PRINCIPLES OF SECURITY

This page intentionally left blank.

CHAPTER 1

PRINCIPLES OF SECURITY

Introduction

0101. This chapter provides a brief summary of the principles of security in the context of personnel security. More detailed information is contained in Chapter 1 of the Defence Manual of Security (DMS) Volume 1 'Protective Security'.

The Definition of Security

0102. Security is the protection of assets and/or people against an unwanted event. The damage arising from an unwanted event is described as compromise.

The Threats to Security

0103. The threats, which are not in priority order, can be summarised as follows:

a. Espionage

b. Subversion

c. Sabotage

d. Terrorism

e. Non traditional

Espionage

0104. A prime area of interest, so far as personnel security is concerned, is the exclusion from access to protectively marked information or material of those people who might become involved in espionage owing to some form of inducement or pressure applied to them, or because of ideological beliefs or disaffection.

0105. Foreign intelligence services (FIS) try to collect information for intelligence purposes and to break through our security defences. They work mainly through agents who are either introduced from overseas or are recruited locally. These agents are known to seek out those with character weaknesses or special circumstances (eg. relatives in countries presenting a special security risk) who can be exploited through bribery, blackmail or other pressures. No one with access, or who may later have access, to sensitive information or material may be considered too unimportant to be cultivated either as a useful contact or possible agent.

Subversion

0106. Personnel may be subject to the threat of subversion by FIS and members of organisations whose interests are inimical to those of HM Government. It may not be easy to detect this form of attack at first sight, so personnel should be alert to disguised approaches.

Sabotage

0107. Sabotage is a threat normally associated with a state of war, with conditions of international tension, or during local internal security situations.

Terrorism

0108. Acts of terrorism may continue to be perpetuated in the UK. The nature of the threat, whether in the UK or overseas, will vary depending on the local situation.

Non Traditional

0109. This covers the compromise of information or assets through, for example, theft, accidental loss, "leaks" and non traditional actions of disaffected staff, fraud and deliberate compromise, corruption or destruction of computer or other data. Such compromise represents a threat to security in its wider sense.

Protective Security

0110. Protective security is maintained by a combination of:

a. **Laws, orders and instructions.** These measures range from the Official Secrets Acts to unit security standing orders.

b. **Physical security measures.** These are covered in Chapter 5 of the DMS Volume 1 'Protective Security'.

c. **Personnel security measures.** These are covered in this volume.

d. **Security education and training.** The aim of security education is to ensure that all who work within the MOD, both military and civilian, irrespective of access, understand both the security threat and their responsibilities for countering it. The aim of security training is to ensure that those individuals who have specific security responsibilities as part of their normal employment are properly trained in their security duties. Security education and training are the responsibility of commanders and line managers at all levels. For details see DMS Volume 1, Chapter 13.

e. **Security survey and inspections.**

'Need to know' and 'Need to Hold'

0111. Knowledge of protectively marked matters must be limited strictly to those who are security cleared to the appropriate level and who need such knowledge in order to carry out their duties. In addition, protectively marked documents must not be retained by individuals unless they are required to hold them for the performance of their duties.

Protective Marking

0112. Assets are protectively marked according to the damage that unauthorised disclosure could cause. An understanding of the Government's protective marking system is required in order to reach the appropriate conclusions about the levels of protection needed in particular circumstances. Guidance on this system is given in Volume 1, Chapter 1 para 0103.

This page intentionally left blank.

BASICS OF PERSONNEL SECURITY

This page intentionally left blank.

CHAPTER 2

BASICS OF PERSONNEL SECURITY

General Security Responsibilites

0201. Everyone in the MOD has a role in the promotion and maintenance of good security. Commanders and line managers at every level are responsible for all aspects of security within their area of responsibility, for ensuring that their subordinates are both aware of their responsibilities and that they carry them out properly. It is equally important that management should be such that only persons who are reliable, responsible and trustworthy have access to protectively marked information and material.

Responsibilities of the Director of Defence Security (D Def Sy)

0202. The responsibilities of D Def Sy are described in Volume 1 Chapter 2.

Responsibilities of Service Commands/TLB Holders

0203. The responsibilities of TLB holders, including Service Commands, are described in Volume 1, Chapter 2.

Responsibilities of Principal Security Advisers (PSyA)

0204. The responsibilities of PSyAs are described in Volume 1, Chapter 2.

Responsibilities for Personnel Security

0205. Following the Security Structures Review (see Volume 1 Chapter 2) arrangements for the exercise of personnel security responsibilities, including management of risk cases, have still to be finalised. In the meantime the following arrangements apply:

a. the Directorate of Defence Security is responsible for civilians in the Central TLB, DPA and Trading Funds and Trading Funds and their non List X contractors, for List X industry (but TLB Holders are responsible for List X contractors employed at their sites), and for categories such as Senior Civil servants and MOD Police officers managed centrally.

b. The single services are responsible for their Service personnel wherever they are employed, for civilians employed in service TLBs (except for categories managed centrally), and for contractors employed at their Service sites.

c. The DLO and PJHQ are responsible for civilians employed in their TLBs (except for categories managed centrally), and for contractors employed at DLO and PJHQ sites.

Contact details for the personnel security staffs are at Annex A to the Introduction.

Responsibilities of the Chief Executive/Defence Vetting Agency (CE/DVA)

0206. CE/DVA is responsible for undertaking, as appropriate, Counter Terrorist Checks (CTC), Security Checks (SC) and Developed Vetting (DV) investigations in respect of all Service personnel including potential enlistments, civil servants in MOD and personnel in the defence industry. The DVA is also responsible for the management of aftercare, as delegated by, or in conjunction as necessary with, the relevant Principal Security Adviser. In addition, it undertakes vetting investigations on behalf of other Government Departments (OGDs).

0207. The owner of the DVA is the Director General Security & Safety (DGS&S)).

0208. The Agency's authority for granting, denying or withdrawing security clearances is given below:

a. **For personnel in industry**

(1) To grant, withdraw or deny security clearances

b. **For Service and civilian employees**

(1) On recruitment

(a) To grant security clearances.

(b) To deny security clearances prior to entry.

c. **In service**

(1) To grant security clearances.

(2) To withdraw security clearance retrospectively from personnel who have been dismissed or administratively discharged in circumstances that amount to a presumption of unfitness for continued clearance.

0209. Where the Chief Executive, in accordance with the guidelines previously agreed with the customer organisations, ie. the relevant Service Command, TLB or D Def Sy, judges the circumstances of a case to be sufficiently contentious, the relevant customer organisation will be consulted. Appropriate arrangements are to be set out in separate Service Level Agreements (SLAs) between the Agency and its customers. The final decision to grant a security clearance in such cases will rest with the customer.

0210. Recommendations for the withdrawal, suspension or denial of security clearances for Service and MOD civilian employees will be referred to the customer for a decision in all cases.

The Aims of Personnel Security

0211. Security in the MOD is based on a number of interlocking procedures, which may not be effective or may even be dangerous if they are applied singly without the support of other measures. Thus, personnel security measures must not be regarded as an end in themselves, but only as a means to an end. In particular, security vetting must be seen as only a part of our protective security system.

0212. Personnel security measures devolve from Government instructions to all departments. They are designed primarily not to catch spies but to exclude or restrict access to protectively marked information or material by persons whose loyalty, reliability or trustworthiness may be in doubt. Also to ensure that those who are appointed to posts which afford access to protectively marked information or material, conduct themselves in such a way as to demonstrate their suitability to retain access.

0213. To achieve these ends, it is most important that any doubts about an individual's loyalty, reliability or trustworthiness are brought to the attention of the security authorities without delay so that, where necessary, action can be taken to limit the risk to security.

0214. In the context of personnel security, although every consideration must be given to safeguarding the rights individuals, in the final analysis, the security of the State must outweigh all other considerations.

Personnel Security Measures

0215. The measures available to achieve an effective personnel security system are:

a. Thorough enquiries into identity, integrity and nationality before recruitment.

b. Security vetting.

c. Supervision of personnel.

d. A system of reporting character defects.

e. Enhanced supervision and containment of people whose loyalty, reliability or trustworthiness is in doubt.

Confidentiality of Information

0216. Recruitment authorities are deemed to be the agents of security vetting organisations in their handling of completed security questionnaires. However, the information provided on such forms is solely for use by security vetting organisations; recruitment authorities are not to take any account of such information in their consideration of a candidate's suitability for actual recruitment.

Personnel Security Correspondence

0217. Correspondence on personnel security matters concerning individuals should always carry a protective marking accompanied by the appropriate descriptor, ie. RESTRICTED – STAFF or RESTRICTED – VETTING, and where necessary be addressed PERSONAL FOR (named authority). Consideration of the need for a higher security marking is the responsibility of the originator.

Rehabilitation of Offenders Acts

0218. In accordance with the Acts stated below, individuals completing the Security Questionnaire (MOD Form 1109) are to declare details of "spent" convictions which may need to be taken into account for the reasons shown:

a. For persons on the mainland of Great Britain – the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975, where national security is concerned.

b. For persons in Northern Ireland – the Rehabilitation of Offenders (Northern Ireland) Order 1978 (Exceptions) Order 1979, where national security or the protection of public safety or public order is concerned.

0219. Any information revealed will be treated in the strictest confidence and will not necessarily disqualify an individual from having a security clearance, but it has to be considered by the security vetting organisation.

Data Protection Act 1998

0220. The Data Protection Act 1998 is about access by individuals to personal data held on them by any organisation. The Act regulates the processing of personal data

and enables the subject of the data to have access to it under certain conditions. The Act covers certain types of manual data as well as automated data. The Act contains a number of exemptions including one for national security. The Secretary of State has signed a certificate under the national security exemption that exempts data that is processed for vetting and intelligence and security investigations and operations from disclosure to the subject and from other provisions of the Act where this is required to safeguard national security. There is a right of appeal to the Information Tribunal, which will hear cases involving national security. The Tribunal will have the power to quash a Ministerial certificate. Further information on the Act is available on the Data Protection website, which can be found under Instructions on the MODWeb, or sought from TLB Data Protection Officers.

0221. Where the Data Protection Act provides subject access rights, for example in respect of criminal records information held by police, these rights are not to be abused by compelling the subject to apply for access, under the Act, to such information for employment purposes. This practice, known as 'enforced subject access' is an offence under the Act. Improper use of information relating to offences may constitute an offence under Rehabilitation of Offenders legislation detailed at para 0218 above.

0222. Spare

Freedom of Information Act 2000

0223. The Freedom of Information Act 2000 relates to the disclosure of information held by public authorities. It is expected that the Act will start to come into force during 2002. The FOI Act is intended to bring about a change in culture towards openness, but there are exemptions to safeguard information that it would not be in the public interest to disclose. Some of these exemptions, such as information relating to national security, are outright exemptions and are not harm-tested. Other exemptions, such as Defence, are protected by a harm test whereby information can be withheld if its disclosure would, or would be likely to, prejudice the interest in question. Applications by the subject for disclosure of personal information will be handled under The Data Protection Act 1998. The Information Commissioner will have wide monitoring and enforcement powers. Appeals against decisions to withhold information will be to the Information Commissioner, or direct to an Information Tribunal in the case of national security information. The Tribunal will consider a departmental decision to withhold information by applying judicial review principles. Further information is available from the FOI website, which can be found under Policy on the MODWeb, or sought from D/Info(Exp)-Access, the lead branch in MOD on FOI.

Official Secrets Acts (OSAs)

0224. Personnel who work for the MOD, see Annex B para 3, are required to complete declaration forms relating to the disclosure of information covered by the OSAs as below:

a. On joining the Department – MOD Form 134

b. On completion of service – MOD Form 135

Offences punishable under OSA 1911 and OSA 1920 are shown at Annex A. A basic guide to OSA 1989 is given at Annex B.

Note: At the time of going to print, the latest editions of the two MOD forms were 134 (3/97) and 135 (1/98).

ANNEX A

OFFENCES PUNISHABLE UNDER EARLIER OFFICIAL SECRETS ACTS (OSAs)

1. **OSA 1911**

a. Section 1 of the Act makes it an offence, broadly, for any person for a purpose prejudicial to the interests or safety of the State, to obtain or communicate information which might be directly or indirectly useful to an enemy.

b. Section 4 penalises attempts and incitements to commit an offence under the Act.

c. Section 7 makes it an offence to harbour a person who has committed an offence under the Act.

2. **OSA 1920**

a. Section 1 of the Act penalises the unauthorised use by any person of uniforms, falsification of reports, forgery, possession or use of forged documents, personation and the making of forged statements, and the unauthorised use or possession of any die, seal or stamp whether real or counterfeit, for any purpose prejudicial to the interests of the State.

b. Section 3 of the Act makes it an offence for any person to interfere with officers of the police or members of Her Majesty's forces in the vicinity of any prohibited place.

c. Section 5 of the Act is concerned with regulation of persons carrying on the business of receiving postal packets and make it an offence for any such person to fail to comply with the provisions of the section or to furnish any false information in connection with the requirements it imposes.

d. Section 6 provides that it shall be the duty of every person to give on demand information as to the commission of offences under the 1911 or 1920 Act and penalises failure to fulfil this duty.

e. Section 7 penalises attempts and incitements to commit offences under the 1911 and 1920 Act.

This page intentionally left blank.

ANNEX B

A BASIC GUIDE TO THE OFFICIAL SECRETS ACT 1989

Background

1. The Official Secrets Act 1989 came into force on 1 March 1990. The 1989 Act replaces section 2 of the Official Secrets Act 1911, under which it was a criminal offence to disclose any official information without lawful authority. Under the 1989 Act it is an offence to disclose official information only in six specified categories, and only if the disclosure is damaging to the national interest.

2. This guide gives answers to basic questions about the 1989 Act. It does not cover everything in the Act, but the respective PSyA should be able to provide more information and advice if needed.

Who is affected by the Act?

3. The Act applies to:

a. **Crown Servants** including –
Government Ministers;
civil servants including members of the diplomatic service;
members of the armed forces;
the police.

b. **Government Contractors** including anyone who is not a Crown servant but who provides or is employed in the provision of goods or services for the purposes of a Minister.

c. A small number of **office holders** and the members and staff of a small number of **non-government** organisations who are Crown servants for the purposes of the Act including –

the UK Atomic Energy Authority;
British Nuclear Fuels plc;
Urenco Ltd;
the National Audit Office and the Northern Ireland Audit Office;
the Offices of the Parliamentary Commissioner for Administration and the Northern Ireland Commissioner.

d. **Members of the Public** and others who are not Crown Servants or government contractors but who have, or have had, official information in their possession.

What is "official information"?

4. This means any **information, document or article** which a Crown servant or government contractor has, or has had, in his or her possession by virtue of his or her position as such.

What are the six specified categories of official information protected by the Act?

5. It is an offence for a Crown servant or government contractor to disclose official information in any of the following categories if the disclosure is made **without lawful authority** and is **damaging**. The categories are:

security and intelligence;
defence;
international relations;
foreign confidences;
information which might lead to the commission of crime;
the special investigation powers under the Interception of Communications Act 1985 and the Security Service Act 1989.

6. Each category may be further defined as below:

a. **Security and Intelligence**: Information about the work in the security and intelligence services.

b. **Defence.** Information about:

(1) The size, shape, organisation, logistics, order of battle, deployment, operations, state of readiness and training of the armed forces of the Crown;

(2) The weapons, stores or other equipment of those forces and the invention, development, production and operation of such equipment and research relating to it;

(3) Defence policy and strategy and military planning and intelligence; and

(4) Plans and measures for the maintenance of essential supplies and services that are or would be needed in time of war.

c. **International Relations:** Information about relations between States, between international organisations or between one or more States and one or more such organisations.

d. **Confidential Information obtained from a State other than the United Kingdom or an International Organisation.**

e. **Crime:** Information, the disclosure of which is such that its unauthorised disclosure would be likely to have any of these effects:

(1) Results in the commission of an offence; or

(2) Facilitates an escape from legal custody or the doing of any other act prejudicial to the safekeeping of persons in legal custody; or

(3) Impedes the prevention or detection of offences or the apprehension or prosecution of suspected offenders; or

f. **Special Investigation Powers.** Information obtained:

(1) By reason of the interception of any communication in obedience to a warrant issued under section 2 of the Interception of Communications Act 1985, any information relating to the obtaining of information by reason of any such interception and any document or other article which has been obtained by reason of any such interception; or

(2) By reason of action authorised by a warrant issued under section 3 of the Security Service Act 1989, any information relating to the obtaining of information by reason of any such action and any document or other article which is or has been used or held for use in, or has been obtained by reason of, any such action.

When is a Disclosure Damaging?

7. The Act sets a different test or tests of damage for the different categories of information. For an offence to be committed under the Act, the disclosure of information must, in general, have damaged the national interest in the particular way, or ways, specified in the Act for the category of official information in

question. It is ultimately for the jury to decide, when the case comes to trial, whether damage has in fact occurred.

When is a Disclosure made without Lawful Authority?

8. Crown servants may disclose official information only in accordance with their official duty. Government contractors may do so only in accordance with an official authorisation or for the purposes of their functions as government contractors and without contravening an official restriction. In any other circumstances a disclosure is made without lawful authority.

What about Members of the Public?

9. If a member of the public – or any other person who is not a Crown servant or government contractor under the Act – has, in his or her possession, official information in one of the protected categories, and the information has been:

a. Disclosed without lawful authority, or

b. Entrusted by a Crown servant or government contractor on terms requiring it to be held in confidence,

it is an offence to disclose the information without lawful authority.

10. It is also an offence to make a damaging disclosure of information relating to security or intelligence, defence or international relations which has been:

a. Communicated in confidence to another State or an international organisation, and

b. The information has come into a person's possession without the authority of that State or organisation.

Is it an Offence to Disclose Means of Access to Protected Information?

11. It is an offence for anyone to disclose official information which it would be reasonable to expect might be used to obtain access to information protected by the Act.

What about the Security and Intelligence Services?

12. For:

a. Present and former members of the security and intelligence services, and

b. People who have been notified in writing that they are subject to section 1(1) of the Act,

it is an offence to disclose, without lawful authority, any official information about security or intelligence. There is no damage test.

Who will be notified?

13. A person may be notified only if his or her work is, or includes, work connected with the security and intelligence services, and the nature of the work is such that the interests of national security require that the person should be subject to section 1(1) of the Act.

Prosecutions

14. In England and Wales, prosecutions for most offences under the Act may be instituted only by or with the consent of the Attorney General. In Northern Ireland they may be instituted only by or with the consent of the Attorney General of Northern Ireland.

What are the Penalties of Unauthorised Disclosure?

15. Offences of unauthorised disclosure under the Act may be tried either on indictment by the Crown Court, or summarily by a magistrates' court. The maximum penalties are two years' imprisonment or an unlimited fine, or both, if the offence is tried on indictment, and six months' imprisonment or a £2000 fine, or both, if the offence is tried summarily.

What about Safeguarding Information?

16. It is also an offence under the Act for a:

a. Crown servant, a government contractor or a notified person to fail to take reasonable care to prevent the unauthorised disclosure of a document or article which is protected by the Act;

b. Crown servant or a notified person to **retain** such a document or article contrary to official duty; and

c. Government contractor or a member of the public to fail to comply with an official direction for the return or disposal of such a document or article.

17. These are summary offences, triable in England and Wales by a Magistrates' court. The maximum penalties are three months' imprisonment or a £2000 fine, or both.

Section 1 of the Official Secrets Act 1911

18. The 1989 Act does not affect the operation of section 1 of the Official Secrets Act 1911, which protects information useful to an enemy. The maximum penalty for offences under section 1 of the 1911 Act is fourteen years' imprisonment.

THE VETTING REGIME

This page intentionally left blank.

CHAPTER 3

THE VETTING REGIME

Introduction

0301. The Review of Protective Security (RPS) completed in 1994 was a fundamental and wide-ranging review of the Government's security policies and practices. It resulted from recognition of the changes in the wider environment in which Government departments and agencies and Government contractors operate, particularly changes in the level and nature of the threats to national security.

0302. In the area of personnel security, the RPS concluded that the vetting process served a useful purpose, not only in disclosing circumstances which might lead to breaches of security, but also as a deterrent to those who might otherwise seek to undermine that security. The Review recommended, however, a new approach to vetting with the greater engagement of line managers and increased openness with staff in post about the outcome of the security vetting process. It also recommended an updated range of checks and security clearances, details of which are given in this chapter.

0303. All candidates for security vetting are to be asked to complete a security questionnaire which will explain the purpose of the procedure and invite them to provide the personal details required for the necessary checks to be undertaken. Vetting will then be carried out on the basis of HM Government's Statement of Vetting Policy at Annex A.

0304. In essence, the purpose of vetting is to exclude those who might be a security risk from having access to protectively marked information or material or to MOD establishments. The process consists of collecting information on individuals and making a judgement based on that information. However, vetting cannot guarantee that a person is totally reliable still less can it give assurance that he will remain so for all time. There is, therefore, a need both for close and continuous supervision by more senior staff of all those who have access to protectively marked assets or to MOD establishments, and for periodic reassessment of security clearances.

Types of Checks and Security Clearances

0305. The vetting regime arising from the RPS comprises;

a. **The Basic Check (BC).** The Basic Check which is a non-security pre-employment check that replaced, in part, the Reliability Check (RC).

b. **The Counter Terrorist Check (CTC).** The Counter Terrorist Check now extended to include a criminal records check.

c. **The Security Check (SC).** The Security Check which essentially replaced Positive Vetting (SECRET) (PV(TS)).

d. **Developed Vetting (DV).** Developed Vetting which effectively replaced Positive Vetting (TOP SECRET) (PV(TS)) and superseded Enhanced Positive Vetting (EPV).

The Basic Check (BC)

0306. The BC is not a security clearance as such, but is a package of pre-employment checks designed to provide a level of assurance of probable reliability. However, since persons on whom a BC has been completed are authorised to have access to RESTRICTED and CONFIDENTIAL material of UK origin, the BC must effectively be regarded as the first step in the overall vetting process. In contrast to security clearances which are processed by vetting staffs, the BC, other than when linked to a criminal records check (see para 0511-0512), is carried out wholly by recruiting staffs. No person may be granted a SC or DV clearance without first having had a BC completed on him, but a security clearance may be sought concurrently with the BC. Full details about the BC and its associated procedures are given in Chapter 5.

The Counter Terrorist Check (CTC)

0307. The CTC is a security clearance but, unlike SC and DV clearances, CTC clearance does **not** authorize persons so cleared **any** access to protectively marked assets. The aim of a CTC is to prevent an individual who has significant connections with terrorist organisations, or who may be vulnerable to pressure from such organisations, from gaining access to information, establishments or material (possibly not protectively marked) which may be of direct assistance to terrorists. It involves the completion of a Security Questionnaire (MOD Form 1109) and a check of counter terrorist and criminal records. Full details about the CTC and CTC procedures are given in Chapter 6.

0308. All persons who may be susceptible to external pressure on account of close Irish, or specific overseas, connections are to be subjected to a CTC before they can be recruited into HM Forces or offered civilian employment with the MOD. Those who subsequently acquire a close Irish, or specific overseas, connection or one with a potential for hostility towards the British Government (for example through marriage) are similarly subjected to the CTC process. The CTC also serves to assist

in the protection of Service personnel, MOD civil servants and their families who may be at risk. A CTC enables an individual to have general, but not specific, access to military or to sensitive establishments.

0309. For the relevance of CTC to persons who unsupervised regularly handle arms, ammunition or explosives or who work as armourers (or equivalent) see para 0610.

The Security Check (SC)

0310. In view of the damage that would result from the compromise of assets attracting higher levels of protective marking, a requirement exists for a level of assurance of integrity beyond that provided by the BC. These higher levels of assurance are provided by two levels of vetting, of which the lower is the SC.

Procedure

0311. An SC clearance involves:

a. A check of departmental records, where they exist.

b. Completion by the individual of a Security Questionnaire (MOD Form 1109).

c. Record checks, including checks against relevant police and Security Service records, and credit reference checks.

d. Where further investigation is warranted, a review of personal finances and/or a subject interview.

0312. Full background about the applicability of financial checks, CRC and FQs, is given at Annex 3C.

Criteria

0313. An SC is required in the following circumstances:

a. For posts involving long-term, frequent and uncontrolled access to assets marked SECRET and those which afford occasional and controlled access to assets marked TOP SECRET.

b. For individuals who, while not in such posts, will be in a position directly or indirectly to bring about the same degree of damage.

c. For individuals being considered for employment where it would not be possible for them to make reasonable progress in their career without clearance to SECRET level.

d. For posts governed by international requirements involving any authorised access to international defence organization (IDO), ATOMIC or special codeword information protectively marked CONFIDENTIAL or SECRET.

e. For crypto-custodians and alternate crypto-custodians requiring access to 10 or less National SECRET keymats.

f. For posts involving any access to NATO or Allied RESTRICTED or CONFIDENTIAL keymats.

See also paras 0329-0330.

Application of Criteria

0314. At SC level, 'long-term, frequent and uncontrolled access' should be interpreted as having unsupervised handling of SECRET material on a regular basis. This could be daily or weekly but should constitute a core function of the post. 'Long-term, frequent and uncontrolled access' also covers access to enough SECRET information to allow an individual to obtain a comprehensive picture of a SECRET plan, policy or project. It will also be required for posts where the holder has **custody** of a small quantity of SECRET material.

0315. In those instances where Service personnel or MOD civilians, who are only BC-approved obtain **inadvertent** or **occasional** access to UK SECRET assets, this is acceptable providing the conditions of para 0507 are fulfilled.

SC Review

0316. MOD personnel and List X Company employees holding SC clearance will be subjected to a review of that clearance at ten year intervals or as required. Similarly, the clearances of persons originally vetted at PV(S) or NV level will be subjected to a review ten years after PV(S) or NV was first granted, or as soon thereafter as is feasible, or as required. The exceptions are Non-List X Company employees and consultants whose clearance will be reviewed every three years, because the aftercare for them is limited.

SC Review Procedure

0317. Details are given in para 0828.

Further Guidance

0318. Specific departmental guidance on the application and maintenance of SC clearances is given in Chapters 8 and 12.

Developed Vetting (DV)

0319. DV is the higher of the two levels of security vetting which authorise those so cleared to have access to protectively marked assets. It is confined to those who have the access and capability to compromise significantly the most sensitive information or operations.

Procedure

0320. A DV clearance involves:

a. A check of departmental records.

b. Completion by the individual of a Security Questionnaire (MOD Form 1109), DV Supplement (MOD Form 1110), and Financial Questionnaire (MOD Form 1117).

c. Record checks, including checks against relevant police and Security Service records and credit reference checks. See also Annex 3C.

d. A review of personal finances. See also Annex 3C.

e. A subject interview.

f. A field investigation which may involve interviews with referees and current and previous supervisors.

Criteria

0321. A DV clearance is required in the following circumstances:

a. For posts involving long-term, frequent and uncontrolled access to assets marked TOP SECRET;

b. For individuals who, while not in such posts, will be in a position directly or indirectly to bring about the same degree of damage;

c. For posts involving authorised access to STRAP TOP SECRET special codeword or special access operation (SAO) information.

d. For all personnel with any access to a hard copy or electronic, individual TOP SECRET keymat (or key variable – KV);

e. For all personnel with access to a complete edition of a current, or reserve, HIGH GRADE NATO or Allied Forces keymat, irrespective of its protective marking;

f. For all personnel appointed as COMSEC Custodian, Accountant or Assistant, having access to 11 or more complete editions of different short titles of national keymats at SECRET level;

g. For posts connected with British diplomatic and consular missions, at the discretion of the Foreign and Commonwealth Office. See also para 0329.

Application of Criteria

0322. "Long-term, frequent and uncontrolled access" should be interpreted as having unsupervised access to assets marked TOP SECRET on a continuous basis, and as an integral part of the post. This excludes:

a. Custody of a small quantity of TOP SECRET material.

b. Occasional access to limited quantities of TOP SECRET material in the normal course of business.

c. Entry to areas where TOP SECRET material is stored.

d. Work in an area where TOP SECRET information might be overheard.

e. Use of equipment capable of handling TOP SECRET material where access control measures are in force, but see para 0321d above.

It follows that SC clearance should be adequate for the conditions listed above.

DV Review

0323. MOD personnel and List X Company employees holding DV clearances will be subjected to a review:

a. Annually - personnel under 21 years of age

b. After five years - for the initial review

- for non List X contractors' staff

- for those holding NATO appointments

c. Every seven years - for subsequent reviews.

The exceptions are List X Sub contractors, consultants and certain volunteer reserve personnel whose clearance will be reviewed every three years, because the aftercare for them is limited. Reviews can be brought forward at any time at the discretion of the appropriate security vetting organisation.

DV Review Procedure

0324. Details are given in para 0923.

Further Guidance

0325. Specific departmental guidance on the application and maintenance of DV clearances is given in Chapters 9 and 13.

The Granting of SC and DV Clearances

0326. A clearance will normally only be granted on the satisfactory completion of the procedures outlined in paras 0310 and 0320. In emergencies, there may be operational demands for access to protectively marked assets to be approved without the required checks. In such cases, it is for the security or the vetting authority, as appropriate, to indicate whether there are any security objections to an individual performing, for a limited time, the duty for which the access is required. Further guidance on the granting of a clearance is given in para 0418, 0804 and 0904.

Refusing Security Clearance – on Recruitment

0327. There is no requirement to inform an individual of the reasons why they have been refused employment with a Government department or agency or List X Contractor. However, where there are specific, clear-cut and non-sensitive reasons for refusing security clearance, the individual may be informed about them, as they may have an impact on any future employment applications. In some cases, considerations of security or confidentiality may prevent explanation.

Notification to Individuals of CTC, SC and DV Clearances

0328. Where clearance has been granted to a member of staff, arrangements should be made locally by the HOE to ensure the individual is informed.

Access to STRAP Material

0329. STRAP is the procedure for the special handling of sensitive intelligence material. The fundamental requirements for access to STRAP information/material are:

a. SC clearance – for STRAP SECRET

b. DV clearance – for STRAP TOP SECRET

0330. For exceptional access to TOP SECRET STRAP material for SC post holders, the STRAP security authority may, on request, grant dispensation where, for urgent operational reasons, it is necessary to permit an SC post holder to have access to TOP SECRET STRAP material. In all other cases for access to TOP SECRET STRAP material, the post holder will require DV security clearance. Further detail is available in Volume 5. See also para 0907.

Access by Dual and Foreign Nationals to National Caveat Material

0331. There are special vetting requirements for MOD civilians (and contractors' employees) with dual nationality, one of which is British, and other foreign nationals who require access to national caveat material. In each case an assessment is to be made by the vetting authority or Principal Security Adviser, as appropriate, as to whether any conflict of interest exists before access is given. Normally a subject interview will be required, but this is not necessary if sufficient information is available to exclude the existence of any conflict. For those cleared to DV level, a subject interview is part of the normal vetting procedure; for those cleared to SC level it is an additional requirement.

0332. By virtue of attestation or equivalent procedures, all Service personnel who have dual nationality, one of which is British, are considered to be British for the purpose of access to national caveat material. There are, therefore, no additional vetting requirements for Service personnel with dual nationality.

0333. Pending the outcome of a review, the Cabinet Office has agreed that the new rules for access to national caveat material for persons with dual nationality should also apply to access to composite caveat material (eg UK/US, UK/GE etc), but see **Note.**

Note: Within the MOD access to composite caveat material is authorised universally subject to the 'need-to-know' principle for Service personnel and for civil servants; for contractors' staff such access may only be granted after the permission of the originator of such material has been secured.

0334. Service, MOD civilian and contractors' personnel with dual nationality, neither of which is British are to be treated as foreign nationals for the purpose of access to caveat material. DMS Volume 1 Chapter 16 sets out the policy on national and composite caveats.

Review on Change of Personal Circumstances

0335. Whenever an individual holding a security clearance, or in the case of non-vetted Service personnel is merely BC-approved, marries, re-marries or sets up a stable unmarried relationship living with someone as a couple, or reports a change of co-residents, there is a requirement for the subject's security clearance/BC approval to be revalidated. It is the responsibility of HOEs to ensure that procedures are established and promulgated to make certain that all personnel are aware of the requirement to report such changes. The procedures for reviews on change of personal circumstances in relation to a CTC, and to SC and DV clearances are outlined in paras 0626, 0828, 0925, 1215 and 1320.

0336. Certain difficulties may arise when a security cleared individual marries or forms a stable partnership with a person of non-UK origin, or to a person normally

domiciled abroad. Depending on the nationality or country of residence involved, such a marriage or stable partnership may cast doubt on the suitability of the subject to retain his current level of clearance or to be granted a higher level of clearance in the future. Personnel entering into such relationships are to be interviewed and advised of the possible security implications. A copy of the interview report, together with the completed Change of Personal Circumstances Questionnaire (MOD Form 1126) is to be submitted to the appropriate DVA unit.

Aftercare

0337. The CTC, SC and DV security vetting processes provide an acceptable level of assurance as to an individual's integrity, and of the appropriateness of their having access to, or knowledge or custody of, sensitive Government assets or information. But vetting *alone* does not provide a guarantee of future reliability. It is, therefore, important that personnel security continues after the initial security clearance has been granted, or in the case of personnel not deemed to require vetting, after BC approval has been given. It is also important that any new information or concerns that may affect the reliability of an individual are brought promptly to the attention of the appropriate authorities. This is achieved through a combination of **aftercare** and security clearance, ie SC and DV review procedures.

The definition of aftercare is given in the introductory chapter para 11a. A full description of HOEs' responsibilities in this sphere may be found in paras 1817 to 1825.

Supplies of Security Forms

0338. Demands for the MOD Forms listed at Annex B are to be submitted to the Defence Storage & Distribution Centre (DSDC(L) 3b) Llangennech. Establishments are to limit their demands to those strictly necessary to meet local requirements. Others forms appearing as annexes to individual chapters are to be reproduced locally with the format and content identical to that shown.

Competing for Quality (CFQ)

0339. Where persons are transferred from the Public Service into CFQ posts their particular level of clearance, ie. BC, CTC or SC goes with them. Full background to the CFQ process is given in the Guide to Competing for Quality in Defence Services 1996. Vetting is covered in Chapter 9.

This page intentionally left blank.

ANNEX A

HM GOVERNMENT'S STATEMENT ON VETTING POLICY

1. In the interests of national security, safeguarding Parliamentary democracy and maintaining the proper security of the Government's essential activities, it is the policy of HM Government that no one should be employed in connection with work the nature of which is vital to the interests of the State who;

a. is, or has been, involved in or associated with any of the following activities:

(1) espionage

(2) terrorism

(3) sabotage

(4) actions intended to overthrow or undermine Parliamentary democracy by political, industrial or violent means; or

b. is, or has recently been:

(1) a member of any organisation which has advocated such activities; or

(2) associated with any such organisation, or any of its members in such a way as to raise reasonable doubts about his reliability; or

c. is susceptible to pressure or improper influence, for esample, because of current or past conduct; or

d. has shown dishonest or lack of integrity which throws doubt on his reliability; or

e. has demonstrated behaviour or is subject to circumstances which may otherwise indicate unreliability.

This page intentionally left blank.

ANNEX B

LIST OF SECURITY QUESTIONNAIRES AND REVIEW GUIDANCE

Ser.	Title	Colour	Form No.	Application
1.	Security Questionnaire	Brick	MOD Form 1109	CTCs
				SC and DV initial clearances
				SC and DV reviews
2.	DV Supplement	Aquamarine	MOD Form 1110	DV initial clearances
3.	DV Supplement (Review)	Mint Green	MOD Form 1112	DV reviews
4.	Financial Questionnaire	Pink	MOD Form 1117	SC initial clearances and reviews as required
				DV initial clearances and reviews
5.	Change of Personal Circumstances Questionnaire	Primrose Yellow	MOD Form 1126	New partner reviews and change of co-residents
6.	Security Questionnaire Review – Guidance	White	MOD Form 1127	SC reviews
				DV reviews

This page intentionally left blank.

ANNEX C

FINANCIAL CHECKS

Credit Reference Checks (CRCs)

1. CRCs are undertaken to confirm a subject's credit status. A company, contracted by the Cabinet Office, is employed to carry out such checks using the following information:

   a. The subject's surname and forename(s);

   b. The subject's full home postal address; and

   c. Any other standard civilian addresses during the previous five years.

2. In response to an enquiry, the company will send the vetting authority a summary and full printout of the relevant data, but will only provide information where there is a 90% or greater probability of matching the details provided by MOD. Unfortunately, the company is **not** able to carry out checks against military or BFPO addresses.

3. Where the information given on the report indicates that there is cause for concern, the subject may be asked to complete a Financial Questionnaire (FQ); this will enable his financial situation to be assessed in greater depth. Individuals will be supplied with the results of the check upon request.

4. Whereas filling in a **Financial Questionnaire** (FQ) is not a formal part of the SC process, its completion is required where:

   a. The subject will have access to particularly sensitive financial assets;

   b. The CRC has been carried out and the results suggest that further investigation is warranted; or

   c. For any reason, a CRC cannot be undertaken.

5. Completion of the FQ will more easily enable the assessor to analyse the subject's financial situation by examining details of a person's finances. In most cases where a CRC has highlighted problems and led to the completion of a FQ, the completed questionnaire should resolve these doubts. However, should misgivings remain, a subject interview should be conducted.

6. For DV clearances completion of a FQ is mandatory.

This page intentionally left blank.

NATIONALITY AND RESIDENCY RULES

CHAPTER 4

NATIONALITY AND RESIDENCY RULES

Introduction

0401. The purpose of this chapter is to provide guidance on the nationality and residency rules affecting Service personnel, MOD civil servants and contractors' employees and the relationship between these rules and security vetting. Whereas 'nationality' is an employment matter governed by external regulations, 'residency' is a vetting issue for which D Def Sy is responsible. The nationality annexes to this chapter are provided for the convenience of users of this manual.

Relationship between Nationality Rules and Security Vetting

0402. Nationality requirements for recruitment are not the same as security requirements, which can be applied to any recruit irrespective of nationality. The purpose of security vetting is to provide an assurance of the loyalty, reliability and trustworthiness of an individual, factors which are not necessarily connected with nationality.

0403. Whilst the fact that a person is not a British national may not of itself be a bar to security clearance, nationality will need to be noted since it may have a bearing on the management of postings. There may also be cases when the subject originates from a country whose interests are inimical to those of the UK and where there is a fundamental conflict of interest which prevents the granting of security clearance. Such conflicts of interest will be addressed on a case by case basis by reference to the relevant Principal Security Adviser during the security vetting process.

The Effects of Nationality at each Vetting Level

Basic Check (BC)

0404. An applicant's nationality does not normally affect the BC process which is explained in detail in Chapter 5 although particular commercial considerations may obtrude. However, there are specific rules for Armed Forces' applicants, currently only in the Army, who do not require any level of vetting on entry. These rules are given at Annex A.

Counter Terrorist Check (CTC)

0405. An applicant's nationality has an important bearing on the CTC since it will be necessary to carry out such checks when an individual has close Irish, or specific overseas, and on occasions, other connections. Full details are contained in Chapter 6.

Security Check (SC)

0406. Nationality considerations affect persons working in and for the MOD in different ways; details are shown below:

a. **Armed Forces** – see Annex B

b. **Civil Service** – see para 0412 below

c. **Contractors' Employees** – see para 0417 below

Developed Vetting (DV)

0407. The nationality rules governing DV are set out as follows:

a. **Armed Forces** - see Annex C

b. **MOD Civil Servants** - see para 0412. Such persons are bound the rules in this paragraph but for those with reserved rights see para 0413.

Special DV Posts

0408. When a person is being considered for a post in the Defence Intelligence Staff (DIS) or a Special Access Operation (SAO) the special nationality rules set out in Annex D apply. For the Government Communications Headquarters (GCHQ) the special nationality and residency rules set out in Appendix 1 to Annex D apply. In managing such appointments it will be incumbent on the posting authority to establish the nationality requirement from the appropriate Principal Security Adviser. If the individual meets the specialist nationality requirements the posting authority will confirm or initiate DV clearance.

Commonwealth and European Economic Area (EEA) Membership

0409. Because nationality requirements differ across the MOD sectors, a full list of Commonwealth members and of member states of the EEA is laid out at Annex E for ease of reference.

Employment Factors relevant to Vetting

Service Personnel

0410. Details of the nationality rules applicable to the recruitment of Service personnel are contained in:

Royal Navy	-	BR689: Naval Recruiting Instructions
Army	-	Recruiting Instructions for the Regular & Reserve Forces
Royal Air Force	-	Standing Instructions for Recruiting Officers (SIROs)

0411. The Armed Forces are not subject to the European Union (EU) Rules on the freedom of movement of workers and employment in the Services has not been open to EEA nationals other than those, for historical reasons, from the Republic of Ireland. Also, although all Service posts require the holder to show special allegiance to the Crown, such posts cannot be designated "Reserved" – see para 0413 below – as the Service incumbents do not exclusively have to be UK nationals.

MOD Civil Servants

0412. On 1 June 1996 the rules were revised nationally. Those governing the MOD apply equally across the Civil Service. Full details are set out in Annex A to Volume 2 of the MOD Personnel Manual. For entry into the Civil Service, nationality considerations will depend on whether an applicant's prospective post is designated "Reserved" or "Non Reserved". Security clearance will be required for "Reserved" posts and may be required for "Non Reserved" posts. Candidates with **dual nationality** (providing that one is an eligible nationality) will be eligible for most posts but may have limitations placed on their actual access to protectively marked and caveated material and their clearance certificates are to be annotated accordingly.

Reserved Posts

0413. Reserved Posts (formerly Public Service posts) are those designated as requiring special allegiance to the State. Candidates for these posts must be UK citizens. Commonwealth and Irish citizens are no longer eligible, although those in post on 1 June 1996 have been granted reserved rights. Aliens may **not** be employed in "Reserved" posts.

Waivers

0414. These will **no longer** be granted for recruitment to "Reserved" posts.

Non Reserved Posts

0415. In addition to UK, Commonwealth and Irish nationals, nationals of other EEA countries and also certain non EEA family members may be recruited to Non Reserved posts (formerly non Public Service posts). The categories of family

members eligible for employment are listed in Annex A to Volume 2 of the MOD Personnel Manual.

Aliens

0416. Non Reserved posts may be filled by an alien holding an **Alien's Certificate.** In this case aliens are defined as those who are neither Commonwealth nor EEA nationals. Annex A to Volume 2 of the MOD Personnel Manual details the recruitment procedures to be followed by Civilian Personnel Management Authorities when obtaining Aliens' Certificates.

Contractors' Employees

0417. The nationality rules applied to the Armed Forces and to MOD civil servants do not generally apply to the security vetting of contractors' employees. Nevertheless, nationality, including dual nationality, will need to be noted since a non British national may experience special conflicts of interest. Accordingly, restrictions on access will need to be considered on a case by case basis.

Residency Rules

General

0418. Unless satisfactory enquiries can be made through *official liaison channels* in the country of origin or other place of residence, candidates should normally have resided continuously in the UK immediately prior to their application for a security clearance for the periods of time stated below:

a.	For Counter Terrorist Check (CTC)	-	three years
b.	For Security Check (SC)	-	five years
c.	For Developed Vetting	-	ten years

In certain circumstances, particularly where an applicant is of UK origin, a shorter period of residency may be accepted and a waiver granted by the relevant Principal Security Adviser. Examples of such circumstances are where the candidate has been:

d. Serving overseas with HM Forces or in some other official capacity as a representative of HMG.

e. Studying abroad or working overseas with a British company.

f. Living overseas with parents.

Further details are set out in Annexes F and G. Exceptionally, residency waivers may be granted to nationals of Commonwealth or EEA countries who do not meet the normal requirements.

Overseas Residency

0419. Paras 0606, 0804 and 0904 provide guidance respectively in relation to CTC, SC and DV. In general, if applicants have residency in a country where the Security Service are able to conduct checks, there should be no bar to a clearance.

This page intentionally left blank.

ANNEX A

APPLICANTS FOR HM FORCES WHO DO NOT REQUIRE SECURITY CLEARANCE ON ENTRY: NATIONALITY AND RESIDENCY CONSIDERATIONS

Nationality

1. To be accepted for non-commissioned service in the Army other than to sensitive employment an applicant should be free from immigration restrictions; have unrestricted rights of entry to, and normally be resident of, the United Kingdom, who is:

   a. a Commonwealth citizen, or

   b. a British Protected person, or

   c. a citizen of the Republic of Ireland

2. The term Commonwealth citizen includes:

   a. a United Kingdom citizen (which embraces those born in UK Sovereign Bases or in British military hospitals overseas);

   b. a British Dependent Territories citizen

   c. a British Overseas citizen;

   d. a British subject under the British Nationality Act 1981, or

   e. a citizen of an independent Commonwealth country.

Residency

3. For this category of applicants there are no residency rules.

This page intentionally left blank.

ANNEX B

APPLICANTS FOR HM FORCES WHO REQUIRE CLEARANCE TO SECURITY CHECK LEVEL: NATIONALITY CONSIDERATIONS

1. To be accepted for service in the Royal Navy, Royal Marines and Royal Air Force or in the Army as an officer, or as a candidate for certain closed employments and trades, ie. as an applicant needing vetting to SC level, a person must satisfy all of the following conditions:

a. That he was born in the UK; or in what is, (or then was) a Commonwealth country or in the Republic of Ireland

b. That at all times since birth he has been a Commonwealth (which includes the UK) citizen, or a Republic of Ireland national

Parents

2. The nationality of a candidate's parents is immaterial when he applies to join HM Forces but, should any enquiry about them prove adverse, this could lead to the subject not being suitable for SC clearance and so being unemployable.

Commonwealth Citizens

3. The term "Commonwealth citizen" includes; a British citizen, a Dependent Territories citizen, a British Overseas citizen, a British subject under the British Nationality Act 1981 or a citizen of an independent Commonwealth country.

Dual Nationals

4. Such personnel may not be enlisted until the recruiting authority has obtained confirmation from the government of the other nation of the dual national that the individual concerned is not liable for national service or for recall to military service with that nation.

Waiver

5. A waiver of nationality requirements will normally be granted by the Secretary of State for Defence for candidates who are British citizens at the time of application, regardless of place of birth or former nationality. In exceptional circumstances, a waiver of the nationality requirements may be granted by the Secretary of State for Defence to applicants who are Commonwealth citizens, or Republic of Ireland nationals, at the time of their application, regardless of place of

birth or former nationality. Any candidate who seeks such a dispensation will have his case considered on its individual merits.

Subsequent DV Clearance

6. When a person holding SC clearance is selected for DV clearance later in his career, the rules in Annex C or Annex D (as appropriate) are to be followed.

ANNEX C

APPLICANTS FOR HM FORCES WHO REQUIRE CLEARANCE TO DEVELOPED VETTING LEVEL FOR GENERAL, NON-SPECIALIST POSTS:

NATIONALITY CONSIDERATIONS

1. To be accepted as a person needing clearance to DV level for employment in the Royal Navy, Royal Marines, Royal Air Force or in the Army, an individual must satisfy all the following conditions:

a. That he was born in the UK, or in what is (or then was) a Commonwealth country or in the Republic of Ireland.

b. That at all times since birth he has been a Commonwealth (which includes the UK) citizen, or a Republic of Ireland national.

c. That each of the candidate's parents was born in such a country or in the Republic of Ireland and has always been, or (if dead) always was, a Commonwealth citizen or a Republic of Ireland national.

Special Nationality Rules

2. A candidate for appointment to certain DV posts must satisfy a more demanding requirement known as the Special Nationality Rules which are set out in full at Annex D and Appendix 1 thereto.

Commonwealth

3. The term "Commonwealth citizen" includes; a British citizen, a Dependent Territories citizen, a British Overseas citizen, a British subject under the British Nationality Act 1981 or a citizen of an independent Commonwealth country.

Dual Nationals

4. Such personnel may not be enlisted until the recruiting authority has obtained confirmation from the government of the other nation of the dual national that the individual concerned is not liable for national service or for recall to military service with that nation.

Waiver

5. A waiver of nationality requirements will normally be granted by the Secretary of State for Defence for candidates who are British citizens at the time of

application, regardless of place of birth or former nationality. In exceptional circumstances, a waiver of the nationality requirements may be granted by the Secretary of State for Defence to applicants who are Commonwealth citizens, or Republic of Ireland nationals, at the time of their application, regardless of place of birth or former nationality. Any candidate who seeks such a dispensation will have his case considered on its merits.

ANNEX D

SPECIAL NATIONALITY RULES

Part I – For all posts, military or civilian, in the Defence Intelligence Staff (DIS)

1. DIS posts are designated as Reserved Posts. This means that, because of the nature of the work, the information or of the material dealt with, the post holders owe special allegiance to the State. DIS posts are therefore open only to UK nationals.

2. DIS posts require that staff posted into them meet the following nationality conditions:

a. They must be British at entry and should have held British citizenship for ten years.

b. They should not have held any other nationality in the last five years.

c. Their surviving parents should be solely British.

d. Any spouse/partner should be solely British.

e. Surviving parents of the spouse/partner should be solely British.

3. Where applicants for DIS posts have not held British nationality for the prescribed periods, or where the family as defined above has a non British nationality connection, a decision will be taken on a case by case basis.

Part II – For posts in a Special Access Operation (SAO)

4. A candidate for appointment to a DV post in the SAO domain must satisfy the following conditions:

a. The subject should hold British nationality.

b. The subject should not be a dual national.

c. The subject's surviving parents should be solely British.

5. The spouse/cohabitant and his surviving parents should also hold British nationality and no other.

6. Members of the subject's immediate family, and any other person to whom the subject is bound by affection or obligation, should not be subject to physical, mental or other forms of duress by a foreign power.

APPENDIX 1 TO ANNEX D

NATIONALITY AND RESIDENCY RULES FOR GCHQ

1. Candidates for employment at GCHQ or the Joint Technical Language Service (JTLS) must satisfy the following rules.

Nationality

2. The subject must be a British citizen (but see Note 1).

3. One of the subject's parents must be a British citizen or have substantial ties with the United Kingdom or, if deceased, have had such citizenship or ties before death. (See Note 2).

Note 1: If the subject holds dual nationality, of which one component is British, he will nonetheless be considered. If successful, the subject will normally be required to give up his non-British nationality as a condition of confirmation of appointment to GCHQ or the JTLS.

Note 2: For this purpose a person has "substantial ties" if:

a. That person holds citizenship of a British Dependent Territory, or is a British Subject by virtue of Part 4 of the British Nationality Act 1981 and has the right of abode in the UK, or holds citizenship of the Commonwealth, the status of a British protected person, EEA nationality or citizenship of the United States of America; **and**

b. That person has a demonstrable connection with the United Kingdom by way of family history or period of residency in, or other service to, the United Kingdom.

General Guidance on Spouses and Cohabitees

4. A candidate married to, or cohabiting with, a person who is not a British citizen remains eligible for employment at the discretion of GCHQ working on behalf of the Secretary of State for Foreign and Commonwealth Affairs. Marriage to, or cohabitation with, a person who is not a British citizen **after** appointment may, in some circumstances, result in a withdrawal of security clearance and transfer to another government Department, or (if this is not possible or the officer does not wish to transfer) dismissal. Each case will be considered on its merits, taking into account the ties between the person involved and the United Kingdom.

Residency

5. Candidates for employment at GCHQ or the JTLS must normally have been resident in the UK for 10 years prior to the date of their application. A candidate may nonetheless be considered if (for example) he has been:

a. Serving overseas with HM forces or in some other official capacity as a representative of HMG.

b. Studying abroad.

c. Living overseas with parents.

6. In such cases, the subject must be able to provide referee cover for the period(s) of residency overseas.

7. The duration of residency overseas and the country(ies) in which residency occurred will also be relevant.

Waivers

8. The Secretary of State for Foreign and Commonwealth Affairs may, at his discretion, waive any of the nationality and residency rules set out above.

ANNEX E

MEMBERS OF THE COMMONWEALTH AND MEMBER STATE OF THE EUROPEAN ECONOMIC AREA (EEA)

Members of the Commonwealth

The United Kingdom

United Kingdom Crown Territories
Channel Islands
Isle of Man

Dependent Territories
Anguilla
Bermuda
British Antarctic Territory
British Indian Ocean Territory
British Virgin Islands
Cayman Islands
Falkland Islands and Dependencies
Gibraltar
Montserrat
Pitcairn, Henderson, Ducie and Oeno Islands
South Georgia & the South Sandwich Islands
(St Helena and Dependencies (principally Ascension and Tristan da Cunha)
Turks and Caicos Islands
The Sovereign base areas of Akrotiri and Dhekelia (areas in Section 2 (1) of the Cyprus Act 1960)

Other Countries
Antigua and Barbuda
Australia
Australian External Territories:
- Australian Antarctic Territory (including MacDonald, Heard and Macquarie Islands)
- Christmas Island
- Cocos (Keeling) Islands
- Norfolk

The Bahamas
Bangladesh (formerly East Pakistan)

Barbados
Belize (formerly British Honduras)
Botswana (formerly Bechuanaland Protectorate)
Brunei
Cameroon
Canada
Cyprus (Republic of)
Dominica
Fiji
The Gambia
Ghana which comprises the former colonies of:
The Gold Coast (including Ashanti)
The Northern Territories of the Gold Coast (a Protectorate)
Togoland (a UK trust territory)
Grenada
Guyana (formerly British Guiana)
India
Jamaica
Kenya
Kiribati (formerly Gilbert Islands)
Lesotho (formerly Basutoland)
Malawi (formerly Nyasaland)
Malaysia which includes:
The Federation of Malaya, comprising the former Crown Colonies of Malacca and Penang and the former Protected states of Johore, Kedah, Kelantan, Negri Sembilan, Pahang, Perak, Perlis, Selangor and Trengganu, Sabah and Sarawak (formerly British North Borneo).
The Maldives
Malta
Mauritius
Mozambique
Namibia
Nauru
New Zealand
New Zealand Territories

a. Colonies and Dependencies:
Niue
Ross Dependency
Tokelau Islands Group (formerly Union Islands)

b. Associate State:
Cook Islands (they have complete internal self-government, but citizens are New Zealand citizens).

Nigeria (including Northern Cameroons)
Pakistan
Papua New Guinea
Seychelles
Sierra Leone
Singapore
Solomon Islands
South Africa
Sri Lanka (formerly Ceylon)
St Christopher and Nevis
St Lucia
St Vincent and the Grenadines
Swaziland
Tanzania (formerly Tanganyika and Zanzibar)
Tonga (or Friendly Islands)
Trinidad and Tobago
Tuvalu (formerly Ellice Island)
Uganda
Vanuatu (formerly New Hebrides)
Western Samoa
Zambia (formerly Northern Rhodesia)
Zimbabwe (formerly Southern Rhodesia and Rhodesia)

Member States of the European Economic Area (EEA)

Austria
Belgium
Denmark
Finland
France
Germany
Greece
Iceland*
Ireland
Italy
Luxembourg
Netherlands
Norway*
PortugalSpain
Sweden
United Kingdom

***Note**:* *Not a member of the European Union

This page intentionally left blank.

ANNEX F

APPLICANTS WHO REQUIRE CLEARANCE TO SECURITY CHECK (SC) LEVEL: RESIDENCY CONSIDERATIONS

1. The residency rule in this context is defined as follows:

Candidates, whether or not they are of UK origin, should normally have resided continuously in the UK immediately prior to their application for a minimum of five years. In certain circumstances, particularly where an applicant is of UK origin or has no UK residency, a shorter period of residency or even no residency may be accepted, where, for example, a subject has:

a. Served overseas on behalf of HMG, in the Armed Forces or in some other capacity; or

b. Lived overseas for study purposes; or

c. Accompanied his spouse, cohabitant or parents overseas.

d. Been a UK national working for a British company overseas.

2. Para 0804 gives clear guidance about enquiries in a subject's country of origin or other place of residency.

Residency Waiver

3. Unless covered under para 1. Above, a waiver of the residency rule by the appropriate Service Command/TLB Holder is required for all candidates who need SC vetting, and who have resided outside the UK for more than a total of 12 months in the five years immediately preceding their application. In the context, however, periods not exceeding 28 days may be disregarded for any calculation of a 12 month period.

This page intentionally left blank.

ANNEX G

APPLICANTS WHO REQUIRE CLEARANCE TO DEVELOPED VETTING (DV) LEVEL: RESIDENCY CONSIDERATIONS

1. The residency rule in this context is defined as follows:

Candidates, whether or not they are of UK origin, should normally have resided continuously in the UK immediately prior to their application for DV clearance for a minimum of ten years. Where an applicant is of UK origin, a shorter period of residency may be accepted where, for example, a subject has:

a. Served overseas on behalf of HMG, in the Armed Forces or in some other capacity.

b. Lived overseas for study purposes.

c. Accompanied his spouse, cohabitant or parents overseas.

d. Been a UK national working for a British company overseas.

2. Para 0904 gives clear guidance about enquiries in a subject's country of origin or other place of residency.

Referees

3. Subjects will be required to provide referee cover for periods of residency overseas. The referees must be British citizens who can be interviewed, preferably in the UK. The duration of a subject's residency overseas and the country(ies) in which the subject has lived will also be relevant.

Residency Waiver

4. A waiver of the residency rule by the appropriate vetting authority Note 1 is required for all candidates who need DV and who have resided outside the UK for more than a total of 12 months in the ten years immediately preceding application. In this context, however, periods not exceeding 56 days may be disregarded for any calculation of the 12 month period.

Eligibility for Consideration of Waivers

5. Candidates with "some" UK residency. A candidate who does not fulfil the residency requirement, but who has resided in the UK may be considered for a

waiver of the residency rule if he has so resided for a minimum of 24 months in the ten years immediately preceding the application.

Note: The waiver rules for GCHQ are different – see para 8 to Appendix 1 to Annex 4D.

THE BASIC CHECK (BC)

CHAPTER 5

THE BASIC CHECK (BC)

Introduction

0501. The report of the Review of Protective Security (RPS) emphasised the importance of an integrated approach to protective security and recommended that:

a. Rigorous checks into identity, integrity and nationality at the recruitment stage would be sufficient, when allied with normal physical security precautions and proper line management supervision, to satisfy the protective security standards at the lower end of the protective marking system.

b. Such checks should be carried out systematically, by recruiting agencies, as a Basic Check (BC).

Separate procedures apply to BCs in industry where long term contracts are involved. Full details are given in Chapter 11. Overall, the BC will impinge most directly on recruiting authorities.

Purpose

0502. The BC is not a formal security clearance. Because of this a person who has been subjected successfully to the BC process is described as *BC-approved*. It is designed to provide a level of assurance as to the trustworthiness and integrity of individuals whose work, in the main, involves *uncontrolled* access to, or knowledge or custody of, government assets protectively marked up to CONFIDENTIAL. This is done by confirming identity and nationality as well as ascertaining to a degree their background and character.

Verification of Identity and Nationality

0503. The key element is to establish that an applicant is who he says he is. The documents necessary to meet this task will vary according to an individual's personal circumstances and/or his nationality. On occasions, the lack of documentation will demand recourse to a photograph signed by a person of some standing in the local community. Full details are given in Annex 5A, paras 2-7.

Verification of Background and Character

0504. The second element is to ascertain something of an applicant's integrity. This is done by a combination of references from past employers and/or academic institutes and from personal referees covering the previous three years. Full guidance is given in Appendix 1 to Annex 5A.

The Need for BC

0505. Though specifically not defined as a level of security clearance, completion of the BC is effectively the first step in the vetting process. Thus, within the MOD, it will be mandatory before employment for:

a. **HM Forces.** All recruits, whether regular or reserve, to the Royal Navy, the Royal Marines, the Army and the RAF.

b. **Civil Service.** All candidates, including casual, temporary and work experience staff.

c. **Cadet Forces.** Prospective Adult Instructors (AIs) wishing to serve with the Sea Cadet Corps (SCC), Army Cadet Force (ACF) or Volunteer Reserve (Training) (VR(T)) and other Air Training Corps (ATC) related staff. (See Note).

Note: In due course, this category of individual and other persons who necessarily work with young persons will become subject to Employment Vetting, the details of which have yet to be determined.

d. **Contractors' Employees.** Those who require unsupervised access to RESTRICTED or CONFIDENTIAL material of UK origin, or unsupervised access to the MOD estate.

e. **Cryptocustodians.** Custodians requiring access to any amount of national RESTRICTED or CONFIDENTIAL keymat. See also para 0313e. and 0313f.

Level of Access

0506. BC approval (see para 0502) allows Service personnel and MOD civilians to have unsupervised access to UK material protectively marked up to CONFIDENTIAL. Access to NATO or to foreign material (including collaborative projects) protectively marked CONFIDENTIAL or higher requires SC level clearance.

0507. From time to time, circumstances arise in which inadvertent or occasional access to UK SECRET assets may occur for Service personnel or for MOD civilians,

who have only been BC-approved. When this happens, those individuals may continue to have that level of access, if SC is not assessed to be necessary, **providing** the commander/line manager/project manager judges that there is a "need to know", gives authority in writing and exercises proper supervision. See also the **Note** below.

Note: The dispensation in para 0507 does not apply to:

a. The employees of List X or Non-List X companies, as they come under the rules set out at para 1120.

b. Persons requiring access to crypto keymat, for which the relevant rules appear at paras 0313e and 0313f.

Existing Non-vetted Personnel

0508. All existing non-vetted Service personnel, both regular and reserve, and existing civil servants are deemed to have had a BC completed on them. This is because the standards previously applied during the recruitment stage closely equate to those formally introduced with the BC process.

Basic Check Verification

0509. It will be necessary for recruiting authorities carrying out the BC process to confirm that BC requirements have been satisfied by completing a Basic Check Verification Record (BCVR), a copy of which is at Annex B. This and the supporting documentation should be retained on the applicant's personal file until he:

a. Withdraws his candidature or is not selected for recruitment.

b. Is put forward for a SC or DV security clearance.

c. Having been recruited, resigns, retires or otherwise becomes "non-effective".

0510. Should an applicant not be enlisted/employed within one year, the BCVR and other supporting papers may be destroyed.

Criminal Records Check

0511. Certain categories, mostly of young persons for whom an added element of background checking is desired, will have their details referred to the National Identification Service (NIS). Referrals must only be made with written dispensation from DDefSy. Referrals to the NIS can only be undertaken by security vetting organisations. Recruiting authorities will have to provide them with full particulars of the individuals concerned. This can best be done using the form at Annex 5C.

Furthermore, the individual will need to sign the declaration at Appendix 1 to Annex 5C acknowledging that a NIS may form part of the BC process. Both forms should be retained on the individual's personal file.

0512. Depending on the output from NIS the respective security vetting organisation will recommend to the recruiting agency whether the individual should be employed. The form at Annex 5C meets this requirement.

Progression to Full Security Clearance

0513. Details of the procedure for submitting cases where an individual requires subsequent vetting to SC or to DV level are given in Chapters 8, 9, 12 and 13.

Limitation of BC Access

0514. A BC once completed and finalised may not be withdrawn. However, if an individual holding a security clearance has it suspended, denied or withdrawn, the individual's access is to be limited to that authorised by the relevant security vetting organisation.

Validity

0515. A BC will need to be completed on individuals before they are employed. However, once employed a BC may not be withdrawn. It remains extant until the holder resigns, retires or otherwise becomes "non-effective". (Career breaks for maternity or paternity leave, even lengthy periods of such leave, do not constitute being "non-effective"). At this level, any security concerns, which arise after an individual is employed, will need to be resolved by management means or treated as matters of discipline. Security vetting organisations will be able to offer guidance to commanders and line managers, as well as to personnel branches and project managers. The BC approval of Armed Forces' personnel who retain a Reserve liability following a period of Regular service remains extant until that Reserve liability expires.

Review on Change of Personal Circumstances

0516. When a serviceman who is non-vetted but BC-approved reports a change in partner, ie. someone with whom he is living as a couple, he is to complete a Change of Personal Circumstance Questionnaire MOD Form 1126. This form is to be sent to the relevant vetting authority for processing.

ANNEX A

GUIDANCE ON HOW TO VERIFY IDENTITY

Introduction

1. The procedures for Basic Checks formalise the enquiries that are carried out as part of the recruitment process to Government service in order to provide a degree of assurance as to the identity and background of a prospective serviceman/employee. An important part of this procedure is ensuring that individuals are who they say they are. Guidance on how to check identity as part of the BC process is given below.

Documents to be Checked

2. Before recruitment, prospective recruits/employees should be asked to provide original documents to establish their identity. Duplicates and photocopies should not under any circumstances be accepted. The documents necessary to establish identity will vary according to the nationality of the individual concerned:-

British Nationals

3. Either a full (10 year) current British passport or, if the subject is over 21, a full passport that has lapsed within the last five years or a combination of at **least two** of the following:

a. **Preferably:**

(1) British driving licence.

(2) P45.

(3) An original long version birth certificate.

(4) An original short version birth certificate which bears an issue date within six weeks of the subject's date of birth.

(5) - Credit card with photograph) accompanied

- Credit card) by three

- Bank charge card and cheque book) statements and signature proof

(6) Proof of residence at a given address, such as a utilities bill (water, electricity, gas or telephone) or a council tax bill.

b. In the absence of any of the above:

(1) Employment references.

(2) Academic records.

(3) Trade and education certificates.

(4) Marriage certificate (where applicable).

(5) Naturalisation certificate (where relevant).

(6) Divorce papers (where relevant).

(7) UK residence permit.

(8) HMF discharge certificate (for recruitment-enlistments).

4. In some instances, particularly where young people are concerned, it may not be possible to fulfil the above requirement. Where this appears genuinely to be a problem the subject should be asked for a passport-sized photograph of himself endorsed on the back with the signature of a person of some standing in the community (eg a JP, medical practitioner, officer in HM Forces, clergyman, teacher, lecturer, lawyer, bank manager or civil servant) and accompanied by a signed statement, completed by the same person, stating the period of time that the subject has been known to him (minimum of three years). The statement should always be checked to ensure that the signature matches that on the back of the photograph and that it contains a legible name, address and telephone number. In all cases of doubt, and for a random sample of the others, the signatory should be contacted, preferably by telephone, to check that he did complete the statement and has known the subject for a minimum of three years.

Other EU Nationals (N/A to recruits for HM Forces)

5. Either a full EU passport or an identity card issued by an EU country.

Other Nationalities

6. Either a full passport issued by the country concerned or a document/letter issued by the Home Office establishing the individual's immigration status in the UK.

7. The following are **not** acceptable as proof of identity:

a. An international driving licence (these are frequently and easily forged).

b. A **copy** birth certificate (such copies can be purchased on request at St. Catherine's House for any identity, not just one's own).

Checking Documents

8. When checking documentation it should be borne in mind that a small proportion of individuals may not be who they say they are. There may be a number of reasons for such deception including:

a. Concealment of a criminal record.

b. Illegal immigration.

c. Concealment of identity for the purpose of terrorism or espionage.

d. Department of Social Security fraud.

9. Any of the above could cause someone to act improperly whilst in government employment (eg commit theft or fraud, breach the Official Secrets Acts, provide false documents for others, threaten the safety and well-being of staff and members of the public). It is thus of considerable importance that care is taken to check documents thoroughly.

10. There are a number of simple steps which can be taken to verify the documents produced:

a. To insist that original documents are produced and not transcripts or photocopies.

b. To examine the documents to ensure that they are originals, especially as modern photocopiers produce excellent results, comparing them where possible with other examples you may have available.

c. To check, as far as possible, that the paper and typeface are similar to any others you may have to hand or may have examined recently and that the watermark, where appropriate, is present. Passports and driving licences invariably contain a watermark.

d. To examine the documents for alterations or signs that the photograph and/or signature have been removed and replaced. An ultra-violet lamp may be useful for this purpose.

e. To check that any signature on the documents tallies with other examples in your possession and, if practicable, ask the prospective employee to sign something in your presence.

f. To check that details given on the documents correspond with what you already know about the individual.

11. You should also note the date of issue of the documents presented to you. Particular care should be taken where documents are recently issued, especially if all the documents available to you are new and there is little referee coverage (see below).

Other Means of Confirming Identity

12. Other means of checking documentation may be available to you and they should not be neglected. For example, adequate referee coverage can provide a high level of assurance, especially where the reference is given by a reputable organisation or by someone known to the recruiting agency. However, reasonable steps should be taken to ensure that the reference is genuine. Written references produced by the prospective employee should be treated with care and, where possible, followed up directly with the organisation concerned, particularly where the reference is less than convincing (eg on poor quality paper or containing spelling or grammatical errors). Where someone, particularly a young person, has difficulty providing both evidence of identity and adequate referee coverage, it may be appropriate to obtain both from the same person (see para 4 above).

Action in Cases of Doubt

13. If, after having examined the information available to you, doubts remain about the identity of a prospective recruit/employee the matter should be referred to the appropriate security staff at TLB/Service Command or Branch level.

APPENDIX 1 TO ANNEX A

GUIDANCE ON VERIFYING BACKGROUND AND CHARACTER

Introduction

1. Where a BC is being carried out as the groundwork for a SC or DV or, in conjunction with a CTC, only one reference is needed. This should be from the individual's most recent employer and should cover a period of one year or be from a previous employer for the same period. If an employer's reference is not available, a personal or academic reference should be obtained.

2. When the individual is being subjected to the BC only, references are required to cover at least the three previous years from two sources:

   a. Previous employers or academic institutes

   b. Personal referees.

An individual's circumstances dictate that a degree of flexibility by recruiting staff is required in their approach to this subject.

References

Previous Employers

3. Ideally, a reference should first be sought from this source. However, since an applicant may have been unemployed for some time, or his previous employer may not be in a position to produce a reference, a second personal reference (see para 4 below) must be obtained. In cases where an applicant has been in HM Forces or the civil service during the past three years, the employer's reference should be sought from his former, immediate superior or line manager, and **not** from the Service or Department.

Academic Institutes

4. Where an applicant has been in full time education during the previous three years, a reference on headed notepaper should be acquired from the relevant school or college.

Personal Referees

5. These are nominated by the applicant. Persons of some standing in the community (see Annex A para 4) should be put forward unless their personal knowledge of the applicant is likely to be insufficient to enable them to provide a considered reference. Where the applicant is unable to nominate a person of standing, a reference should be obtained from personal acquaintances who are not related to, or involved in, any financial arrangement with the applicant.

Young Persons as Applicants

Identity and Referee Coverage

6. Where someone has difficulty in providing adequate evidence of both, it may be appropriate to obtain both from the same person.

Dearth of Referees

7. Exceptionally, in those instances where referees are found to be in short supply, the recruiting authority should apply to its respective personnel authority for dispensation.

ANNEX B

BASIC CHECK VERIFICATION RECORD (BCVR)

1. **APPLICANT/EMPLOYEE DETAILS**

Surname:……
Forenames:……

Address:……
……Tel:……
…….Date of Birth:…… Place of Birth:……. Nationality:……
Former or dual nationality:…….. (with dates if applicable)
(with dates if applicable)

2. **CERTIFICATION OF IDENTITY**

Document	Date of Issue
a.	
b.	
c.	
d.	

3. **REFERENCES**

Referee	Address	Relationship	Length of Association
a.			

b.			

4. **OTHER INFORMATION (eg Criminal Record Declaration)**

5. I certify that, in accordance with Chapter 5 of the Defence Manual of Security Volume 2 – Personnel Security, I have personally examined the documents listed at para 2. above and have satisfactorily established the identity of the above applicant/employee and that I have obtained the references and information listed at paras 3. and 4. above and that these references satisfy the requirements.

6. In addition, I have seen the following (academic certificates etc.):

Name: Post:

Signature: Date:

ANNEX C

RESTRICTED – STAFF (when completed)

To: Respective DVA Unit

From: Address of Recruiting Agency, MOD sponsor or ESyO for Non List X company.

Application for a NIS Check for a Civilian Employee

PART 1

(Unit)……..

SURNAME……. (Male/Female) delete as necessary.

First names in full…….

Date of Birth…….

Company name (if contractor's staff)……

Country and place of birth……

Previous surnames used…….

Private address…….

…….

Previous address/es over last five years……

…….

…….

1. S/he has been subjected to a Basic Check (BC). Adverse information resulting from the BC should be attached to this application.

2. To complete the extended BC process required for this appointment, please arrange for a NIS check to be carried out.

3. The above person has given written permission for the check to be made and is aware that any 'spent' convictions will be disclosed.

Date:

Signature:
Name:
Tel:

RESTRICTED – STAFF (when completed)

RESTRICTED – STAFF (when completed)

PART II

To: Vetting Enquiry Office
National Identification Service
Room 336
New Scotland Yard
Broadway
London SW1H 0BG

1. Would you please conduct an NIS check for national security purposes on the person whose particulars appear at Part I.

2. I am satisfied that the particulars given are accurate and that the above named person has given written permission for the check to be made and is aware that any spent convictions will be disclosed.

3. I certify that this request for conviction information is for a purpose which has been authorised by the Association of Chief Police Officers.

Vetting Unit Stamp

Signature

Date

PART III

Subject……

Proposed Post……..

4. In respect of the person named in Part I EITHER: (Delete a. or b. as necessary.)

a. NIS check completed and no significant traces found; OR

b. We recommend that the person should NOT be employed in the post specified above. This is not to say that the person is unsuitable for employment in an alternative post. You are reminded that in the case of prospective employees, you are not required to inform the person why s/he is not being taken on.

Vetting Unit Stamp

Signature

Date

RESTRICTED – STAFF (when completed)

APPENDIX 1 TO ANNEX C

Address of Recruiting Agency,
MOD sponsor (or ESyO) for Non List X company

PERSONAL DECLARATION

Surname…….Date of Birth……..
First Names in full……..Place of Birth…….
I understand that the recruiting process may involve a criminal record check which will, if undertaken, be conducted on the grounds of national security and result in any 'spent' convictions held against me being disclosed on a strictly in confidence basis to the MOD security vetting organisation for assessment.

Signature

Date

Note: This declaration is to be retained on the individual's personal file held by personnel management once it has been signed.

This page intentionally left blank

THE COUNTER TERRORIST CHECK (CTC)

CHAPTER 6

THE COUNTER TERRORIST CHECK (CTC)

Introduction

0601. The Counter Terrorist Check (CTC) is a level of security clearance. However, unlike SC and DV, CTC clearance does **not** provide access to protectively marked information or material. A CTC is required to be carried out in the interests of national security before anyone can be:

a. Granted unescorted access to those military, civil and industrial establishments assessed by the relevant Service Command/TLB to be at particular risk of attack by terrorist organisations; or

b. Authorised to take up posts which involve proximity to public figures at particular risk of attack by terrorist organisations or which give access to information or material assessed to be of value to terrorists.

0602. The CTC is designed:

a. To prevent those who may have connections with terrorist organisations, or who may be vulnerable to pressure from such organisations, from gaining access to certain posts and, in some circumstances, premises where there is a risk that they could exploit that position to further the aims of a terrorist organisation.

b. To provide information to ensure that serving officers, servicemen and MOD civil servants, together with their families, who may be at risk by having close Irish, or specific overseas, connections can be protected.

Procedure

0603. A CTC entails the completion of a Security Questionnaire (MOD Form 1109), confirmation of identity and a check of both counter terrorist and police records.

Vetting Authority

0604. The DVA is responsible for granting CTC clearances.

Nationality

0605. The nationality rules governing eligibility for employment within MOD are set out in Chapter 4.

Residency

0606. General guidance is given in para 0418. Vetting authorities may however exercise discretion having regard to the total coverage which has been achieved. In certain circumstances, particularly where an applicant is of UK origin, a shorter period of residency may be accepted, subject to a waiver being granted by the vetting authority.

Access

0607. A CTC may be required as a condition of unescorted access as defined in para 0601a above. HOEs are to ensure that a CTC is carried out before an individual is employed in a post giving access to any of the following:

a. Information relating to policies or operations designed to counter the threat from terrorist organisations, where the level of access to protectively marked information does not meet the criteria for carrying out a Security Check (SC) or Developed Vetting (DV) clearance.

b. Information or material which may be of direct assistance to terrorist organisations in targeting or carrying out terrorist attacks, such as may be gained from access to sites or proximity to public figures at particular risk of attack.

Link to Basic Check and Security Clearances

0608. The CTC is incorporated into SC and DV clearances but it is wholly independent of the Basic Check (BC). The grant of CTC clearance does not authorise a person to have access to protectively marked material. Should a CTC cleared individual require access to RESTRICTED or CONFIDENTIAL material of UK origin, this will be permissible on receipt of BC clearance, subject to application of the "need to know" principle. When an individual holds a valid SC or DV clearance, or a request for such a clearance has been initiated, there is no need to seek a CTC.

Application to Service Personnel and Civil Servants

0609. All potential recruits to the Services, both regular and reserve, and to the Civil Service who do not require a SC or DV clearance as a prerequisite to recruitment, are to be required to complete a security questionnaire (MOD Form 1109). Once completed, the questionnaire is to be examined by the appropriate recruiting authority or establishment security officer (ESyO) or project manager in accordance with para 0613. If a CTC is then needed, it is to be regarded as a prerequisite for the individual's recruitment.

Application to Weapons/Ammunition/Explosives Handlers

0610. All personnel, whether military, civilian or contract, whose duties involve regular, unsupervised access to weapons, ammunition or explosives are not to assume such duties until they have been subjected to a BC and CTC clearance. Where the responsible Service Command/TLB considers it justified, the vetting requirement may be changed to SC level.

0611. Where persons currently engaged in such duties do not hold at least BC and full CTC clearance, priority action should be initiated to achieve that level of security clearance.

Application to Contractors' Employees and Other Visitors

Regular and Long Term Visits

0612. All contractors' employees and visitors to military establishments who require unescorted access and whose visit(s) will either comprise one visit of more than two weeks' duration or several visits which total more than two weeks within any six month period are required to complete a Security Questionnaire (MOD Form 1109) which is to be examined in accordance with para 0613. Exceptionally, should circumstances arise in which contractors are unable to carry out their work owing to their staff not having security clearances, the Principal Security Adviser may consider granting a waiver or even an exemption. Both of these measures authorise a deviation for varying periods of time from the normal, mandatory standards. Full details of these procedures are contained in Volume 1, Chapter 2, Waivers and Exemptions.

0613. Persons who require unescorted access to areas used to store arms, ammunition and/or explosives or to areas occupied by people who could constitute an attractive target for terrorists are to be subjected to this procedure irrespective of the length of their proposed visit. Where a CTC is required, heads of establishments are to ensure that those concerned are not given unescorted access to their establishment until the CTC has been completed satisfactorily.

Irregular and Short Term Visits.

0614. Casual visitors or contractors' employees whose business at a military establishment is for a period of less than two weeks and who are not security-cleared, may be granted access if escorted by Service or Civil Service personnel. They may be granted **unescorted** access, providing:

a. A genuine reason for the visit has been positively established, ie the individual has been officially invited to attend or has some statutory or official power to enter.

b. They are not allowed access to areas where sensitive information of value to a terrorist (such as personnel records) could inadvertently be compromised.

c. They will not have access to arms, ammunition and/or explosives or unauthorised access to Service offices, domestic accommodation and messes. In the above circumstances, the requirement to complete a security questionnaire may be put aside in favour of filling in a local access control proforma.

The general regulations for control of entry are contained in Volume 1, Chapter 5, Section IX. See **Note** below

Note: The provisions contained in para 0614 do not apply to Central TLB, DPA and Trading Fund establishments.

0615. Further information is contained in Chapter 14.

The Requirement for a CTC

0616. Once a security questionnaire has been completed by a prospective recruit, a contractor's employee or a potential visitor, the recruitment authority, ESyO or project manager is to examine the information provided. A CTC is required in the following circumstances:

a. **Close Irish Connections.** Whenever there is an indication of any connection by place of birth or place of residence with Northern Ireland or Eire, in respect of either the subject, his spouse or his close relatives. Full definitions of close Irish connections and of close relatives in this context are given at Annex A.

b. **Specific Overseas Connections.** Whenever there is an indication of any connection by place of birth or place of residence with any country or organisation that has the potential for hostility towards the British

Government. Further background on this aspect is given at Annex B. No country within the commonwealth or the European Economic Area is deemed to pose a threat.

c. **Persons Attracting Security Attention.** Whenever a person comes to notice after enlistment/employment (eg. as a result of a security investigation, report etc.) as possibly having close Irish, or specific overseas, connections.

d. **Defence Procurement Agency.** For all DPA contracted List X and Non-List X Company employees needing unescorted access, unless special dispensation has been granted by the DPA.

0617. A CTC is not required for dependants of SC or DV cleared Service personnel and civilian staff unless the dependant concerned has close Irish, or specific overseas, connections.

0618. If recruiting authorities or establishment security staffs are ever in any doubt as to whether a CTC is required they are to consult the Principal Security Adviser (Annex Intro A-1) on matters of policy and the vetting authority on any specific vetting issues.

Clearance Action

0619. Once the requirement for a CTC has been identified by the appropriate authority, cases are to be processed under the agreed administrative procedures for each Service Command's/TLB's area of responsibility, ensuring that the confidentiality of the information provided by the individual is protected at all times.

Timescale

0620. A CTC generally takes four to six weeks to complete from the date of receipt of the correctly completed security questionnaire at the vetting authority but may take up to four or more months.

Disposal of Completed Questionnaires

0621. If a CTC is not required at recruitment, the completed Security Questionnaire should be retained for one year after which it may be destroyed. When a CTC is not required but the individual is granted access to an establishment, the ESyO is to retain the completed questionnaire for the duration of such access.

Validity of CTC Clearance

HM Forces and Civil Service

0622. If a recruit or a civilian applicant who has been CTC cleared has not been enlisted/employed or recruitment-enlisted/recruitment-employed within six months of being so cleared, a CTC on him will be repeated. A person who has been CTC cleared will retain that level of clearance subject to any revalidation until he retires, resigns or otherwise becomes non-effective. See also para 0624.

CTC Aftercare and Reviews

0623. The personnel security process continues after a CTC clearance has been granted; connect para 0337. Aftercare arrangements are outlined in paras 1817 – 1824 and Sectors should have implemented the necessary procedures with effect from 1 April 1998.

0624. CTC clearances reviewed as under:

a.	HM Forces and Civil Service	-	every ten years
b.	Non-List X contractors' employees	-	every three years
c.	List X contractors' employees	-	every ten years
d.	List X sub contractors' employees	-	every three years

0625. Spare.

Review on Change in Personal Circumstances

0626. When an individual who holds a valid CTC reports a change in partner, ie someone with whom he is living as a couple, he is to complete a Change of Personal Circumstances Questionnaire (MOD Form 1126), which is to be subjected to the CTC assessment procedure outlined in para 0613. Where this process shows a requirement for the new partner to be subjected to a CTC the questionnaire is to be submitted to the vetting authority under the agreed administrative procedures for each Service Command/TLB ensuring that the confidentiality of the information provided by the individual is protected at all times.

ANNEX A

DEFINITION OF CLOSE IRISH CONNECTIONS

1. A potential member of HM Forces or a prospective or serving MOD civil servant or a contractor's employee is deemed to be inherently vulnerable to pressure from terrorist organisations if he has close Irish connections ie.

a. Was born in Northern Ireland (Note 1) or in the Republic of Ireland, or

b. Resides in, or has resided in, Northern Ireland or the Republic of Ireland within the last five years (excluding Crown Service, but not UDR or R IRISH "Home Service" in the Province) or

c. Has a close relative who was born or resides, or has in the last five years resided, in Northern Ireland or in the Republic of Ireland.

d. Has, or has had, a close association, eg. a fiancee, cohabitant etc with an individual who was born or resides, or has in the last five years resided, in Northern Ireland or in the Republic of Ireland.

2. The term "resided in Northern Ireland" is taken to embrace any address in Belfast or in the counties of Antrim, Armagh, Down, Fermanagh, Londonderry or Tyrone (see Note 1).

Definition of a Close Relative

3. A close relative in the context of para 1 above will generally only include the co-habitant and the subject's parents.

4. There may be circumstances when it may be necessary to investigate a subject's background more widely.

Note: A person is NOT considered to have close Irish connections if he happened to be born in Northern Ireland only because his parents were serving there on Crown Service at the material time.

This page intentionally left blank.

ANNEX B

DEFINITION OF SPECIFIC OVERSEAS CONNECTIONS

1. An individual is considered to be potentially vulnerable to pressure from specific overseas connections if any of the following conditions apply:

   a. He has previously lived, or worked, in a country which harbours, or is sympathetic to, a terrorist organisation which is hostile, or potentially hostile, towards the British Government and/or

   b. In certain circumstances he has close relatives or friends with whom he is in regular contact who live in a country which harbours, or is sympathetic to, a terrorist organisation which is hostile, or potentially hostile, towards the British Government.

2. Countries which harbour, or are sympathetic towards, terrorist organisations that may be hostile towards the British Government and the terrorist organisations themselves may well alter as time goes by. However, persons will possess specific overseas connections, if they are linked with countries that:

   a. Are involved, or are suspected of being involved, in anti-British terrorism or

   b. Have a potential for hostility towards the British Government.

3. Further guidance may be found at Annex A to Chapter 21. This lists those countries to which Special Security Regulations Apply (CSSRA). Perusal of it, when related to current events, will give a good indication as to which countries fall into those categorised at para 2 above.

4. If persons working within the military recruiting organisation, within the civilian personnel management authorities (CPMAs) or as sponsors supervising contractors' employees are in any doubt about the status of a particular country, advice should invariably be sought from the relevant Principal Security Adviser, which in turn may seek guidance from D Def Sy.

This page intentionally left blank.

CHAPTER 7

(SPARE)

This page intentionally left blank

SECURITY CHECK OF SERVICE AND CIVILIAN PERSONNEL

CHAPTER 8

SECURITY CHECK OF SERVICE AND CIVILIAN PERSONNEL

Purpose and Procedures

0801. The purpose of the Security Check (SC) and the procedures for carrying out SC clearances are set out in paras 0310 and 0311.

Vetting Authority

0802. The vetting authority responsible for SC clearances is the Defence Vetting Agency.

Nationality

0803. The nationality rules governing eligibility for employment within MOD are contained in Chapter 4.

Residency

0804. General guidance is given in para 0418. Vetting authorities may exercise discretion having regard for the total coverage which has been achieved. In certain circumstances, particularly where an applicant is of UK origin, a shorter period of residency may be accepted, subject to a waiver being granted by the vetting authority.

Criteria

0805. The criteria covering the requirement for SC clearance and the application of the criteria are contained in paras 0313 and 0314.

0806. Heads of establishments (HOE) are to ensure that personnel are cleared to SC level before they are granted access to protectively marked information and assets to the levels specified in paras 0313 and 0314.

Pre-entry Requirements

0807. Personnel in the areas and categories listed below are required to be SC cleared prior to recruitment or enlistment.

a. **Royal Navy**

(1) All regular RN and RM personnel.

(2) All RNR and RMR personnel.

(3) Retired RN and volunteer reserve personnel nominated for dormant appointments.

(4) Retired RN officers recruited to fill Retired Officer (RO) billets.

(5) RFA and RMAS employees.

(6) Most non-industrial civil servants including all civilian security officer (CSO) grades.

(7) Industrial civil servants recruited to fill specific SC annotated posts.

b. **Army**

(1) All officer entry candidates for commissions in the Regular or Territorial Army.

(2) Soldier entrants recruited for certain closed trades and units.

(3) Retired Officers recruited to fill RO grade appointments.

(4) Certain non-industrial mobile grade civil servants including all civilian security officer (CSO) grades.

(5) Industrial civil servants recruited to fill specific SC annotated posts.

c. **Royal Air Force**

(1) All regular RAF personnel.

(2) All auxiliary and volunteer reserve RAF personnel excepting members of the RAFVR(T) and unsponsored members of University Air Squadrons.

(3) Retired RAF Officers holding RO grade and war appointments.

(4) University cadets and bursars.

(5) Non-industrial civil servants including all civilian security officer (CSO) grades.

(6) Industrial civil servants recruited to fill specific SC annotated posts.

d. **Central TLB, DPA and Trading Funds.**

All civilian staff with two **exceptions**:

(1) The Meteorological Office, which in certain circumstances is allowed to employ staff who are only BC approved, with SC clearance being applied for as soon as practicable after recruitment, and

(2) The Pay & Personnel Agency which has been specially authorised to employ clerical staff having only BC approval and CTC clearance.

Clearance Prior to Employment

0808. It is the responsibility of the recruiting authority to carry out the BC to initiate and obtain SC clearance and to bring to the attention of the vetting authority any information of potential security significance that emerges during the recruitment process.

0809. When SC clearance is a pre-employment requirement the recruiting authority must possess a notification of SC clearance before actual recruitment or enlistment.

0810. For the relevance of SC to unsupervised persons handling weapons, ammunition or explosives see para 0610.

0811. The aim should be to grant SC to prospective recruits within six months of the procedure being started. If unforeseen delays occur that extend the procedure to not longer than under one year, the candidate must be asked to re-sign and re-date the Declaration on MOD Form 1109 and to enter the following statement on page 10 or 11 as appropriate.

"I hereby certify that since I initially completed the questionnaire there have been no changes to the information which I provided then."

Note: Should minor changes have taken place, such as a change of name following marriage, this is acceptable providing the latest details have been entered, initialled and dated.

Clearance of Existing Personnel – Royal Navy, Army and Royal Air Force

0812. If SC clearance has to be initiated for existing personnel, the Service posting or personnel authority or civilian personnel management authority (CPMA) is responsible for initiating SC clearance action.

Clearance Action – Service Personnel

0813. Working to the agreed administrative procedures for their Service, and ensuring that the confidentiality of the information provided by the individual is protected at all times, recruiting or initiating authorities are to arrange for the subject to complete the Security Questionnaire (MOD Form 1109) and then submit it to the DVA:

Royal Navy	-	RN Form S2600 for serving personnel
Army	-	AF B6701 for new recruits
	-	AF B6703 for serving personnel
Royal Air Force	-	Form DV10D for serving personnel

0814. SC clearance may be sought concurrently with the BC but a clearance cannot be granted until confirmation has been received that the BC has been satisfactorily completed.

Clearance Action – Civilian Staff

0815. CPMAs or initiating authorities are to arrange for the subject to complete the Security Questionnaire (MOD Form 1109) and place it in the envelope provided and return it, sealed, with any other documentation to them for onward transmission to their vetting authority under cover of the request for clearance form at Annex A.

0816. SC clearance may be sought concurrently with the BC but a clearance cannot be granted until confirmation has been received that the BC has been satisfactorily completed. Should the applicant withdraw for any reason, the vetting authority should be informed.

0817. If there is evidence of serious illness or mental instability the case must be referred to the British Medical Institute/Civil Service Occupational Health Unit to

obtain a medical opinion of fitness for employment and security clearance before submission to the vetting authority.

Timescale

0818. SC clearance will normally take between four to six weeks to complete, from date of receipt of the correctly completed security questionnaire at the vetting authority, but it can take longer, especially where Irish or specific overseas enquiries are involved.

Notification

0819. The vetting authority will notify the initiating authority or establishment of the granting or denial of SC clearance. Where clearance has been granted to a member of staff, arrangements should be made locally by the HOE to ensure the individual is informed.

0820. If an SC cleared potential recruit is not employed, the clearance notification is to be retained by the recruiting authority for a minimum of six months after the date of issue and is then to be disposed of under agreed arrangements. The vetting authority is to be informed using the tear-off slip where provided when the employment option has been taken. See also para 0811.

Restrictions – Young Persons

0821. Personnel under 21 years of age may be granted SC clearance. However, whilst under 17 years of age they should not normally be allowed access above CONFIDENTIAL.

Limitation of Clearance

0822. Where it has been decided that a person's level of access is to be below that authorised for SC, the HOE is to be informed and the personnel authority given any necessary guidance on the individual's future employment.

Validity of Clearance

0823. SC clearance has replaced PV(S) clearance which previously replaced NV clearance. PV(S) and NV clearances remain valid for ten years or until the individual resigns, retires or otherwise become ineffective. An SC clearance will remain valid for ten years (see para 0316) or until resignation or retirement, except where it is withdrawn or suspended, or lapses prior to recruitment (para 0810) or when no longer required. It may require revalidating when an individual returns to duty after a period of absence of twelve months or more.

0824. SC clearances for the categories of staff in the Central TLB, DPA and Trading Funds set out below only remain valid for the periods specified after which the whole clearance procedure is to be repeated, if required.

a. Student and graduate engineers, student scientists, graduate retraining scheme, mid-term sponsorship scheme and senior research fellows for the period of their studies.

b. College based sandwich course students and bursaries for the period of attachment.

c. Cooperative awarded science and engineering students for the period of study.

0825. When civilian staff, who are in possession of SC clearance, cease to require the clearance because of transfer, resignation etc the vetting authority is to be notified of the full name, date of birth, status and date of cessation of requirement for the clearance. In the case of the transfer of a civilian employee, the name is required of the receiving department.

Aftercare

0826. The personnel security process continues after a clearance has been granted. Aftercare arrangements are outlined in paras 1817 – 1824.

SC Review

0827. SC clearances will be reviewed as specified in para 0828. Responsibility for initiating the review of an SC clearance rests with:

Royal Navy	-	DVA for RN personnel and CPMA for civilian staff.
Army	-	DVA for Army personnel and civilian staff.
Royal Air Force	-	Station Security Officers.
Other TLBs	-	DVA.

Procedure

0828. A SC review involves:

a. Providing the individual with a copy of a Security Questionnaire (Review) Guidance (MOD Form 1127), and then asking him to update his personal details by completing MOD Form 1109.

b. A check of departmental records.

c. A further NIS check and credit reference check.

d. A check with the Security Service, only if there has been a change of partner or of step-parent since the initial clearance or last review, or if the individual had previously been subjected to Normal Vetting (NV) as opposed to PV(S) or SC clearance.

e. Where further investigation is warranted, a review of personal finances.

Review on Change of Personal Circumstances

0829. A SC clearance is to be revalidated if the subject marries, remarries or sets up a stable unmarried relationship living with someone as a couple, or reports a change of co-residents. Personnel holding a SC clearance who report such a change in their circumstances are to be asked to complete a Change of Personal Circumstances Questionnaire (MOD Form 1126). Cases are to be processed under the agreed administrative procedures for each Service/TLB ensuring that the confidentiality of the information provided by the individual is protected at all times.

Clearance of Locally Engaged Civilians Overseas

0830. Locally engaged civilians overseas may require SC clearance. Details are given in Annex B.

This page intentionally left blank.

ANNEX A

RESTRICTED – STAFF (When completed)

To: [Vetting Authority] From: [Establishment]

Ref: [Establishment ref] Date:

REQUEST FOR SC CLEARANCE PROSPECTIVE*/EXISTING* CIVILIAN EMPLOYEE

Name:……..Present post/establishment:……

Grade:……..Proposed post/establishment:……

1. The above named is being considered for employment in the named post* /a general vacancy* requiring SC clearance. This is a RESERVED*/NON RESERVED* POST.

2. The completed security questionnaire is enclosed.

3. It is certified that:

a. For new entrants:

(1) *A Basic Check has been completed and a Basic Check verification record (BCVR) is attached; OR

(2) *A BCVR will be forwarded on completion of the Basic Check.

(3) A health declaration has been completed.

There is no evidence of any potentially adverse information or of serious illness or mental instability* /the following potentially significant factors have been revealed* (copies of relevant papers are attached):

_____

_____

b. For existing staff:

(1) The subject's management files are enclosed*/will be forwarded*

(2) I know of no aspects of the subjects character, conduct or professional competence that would make him/her unsuitable for SC clearance.

Signed…….. (To be signed by EO or above)

Name……(Block Capitals)

Rank/grade……

Tel No and ext……..*Delete as necessary

This page intentionally left blank.

ANNEX B

CLEARANCE OF LOCALLY ENGAGED CIVILIANS OVERSEAS

1. Locally engaged civilians (LEC) fall into three categories:

   a. Dependants of UK based civil servants (UKBCS) or of Service personnel employed in the Command.

   b. Other locally resident British civilians.

   c. Aliens.

Dependants of UKBCS or Service Personnel employed in the Command

2. Such persons may be authorised access as under:

   a. Unsupervised, up to UK CONFIDENTIAL, providing they have been subjected to a Basic Check (see Chapter 5) and to local checks made under Command arrangements.

   b. Occasional and controlled, up to UK SECRET, providing they have been screened locally and, where relevant, subjected to UK checks (see para 4).

3. Where the higher level of access is required, a completed security questionnaire is to be forwarded to the vetting authority accompanied by the results of local checks.

4. UK Checks may be carried out if the individual has:

   a. Served in HM Forces during the previous ten years

   b. Resided in the UK for six months or more during the previous five years.

In such cases, the security questionnaire is to be clearly marked on the top of the front cover in red “For UK Checks”.

Other Locally Resident British Civilians

5. In the absence of suitable dependants of either UKBCS or servicemen, locally resident British citizens should be considered for employment since they can

readily be subjected to a Basic Check, local checks and, when applicable, to UK checks.

Aliens

6. Except when dispensation has been given, the overall aim should be to confine access to UK information/material protectively marked CONFIDENTIAL or above to British citizens of UK origin. To fill particular posts it may be necessary to employ aliens, in which case the rules to be followed are laid down in Chapter 3 of the Recruitment Volume of the MOD Personnel Manual. In such instances the responsibility for authorising and controlling access to protectively marked material lies with the overseas Command.

DEVELOPED VETTING OF SERVICE AND CIVILIAN PERSONNEL

CHAPTER 9

DEVELOPED VETTING OF SERVICE AND CIVILIAN PERSONNEL

Purpose and Procedures

0901. The purpose of Developed Vetting (DV) and the procedures for carrying out DV clearances are set out in paras 0319 and 0320.

Vetting Authorities

0902. The vetting authority responsible for DV clearances is the Defence Vetting Agency (DVA).

Nationality

0903. The nationality rules governing eligibility for employment within MOD are contained in Chapter 4.

Residency

0904. General guidance is given in para 0418. Vetting authorities may, however, exercise discretion having regard to the total coverage which has been achieved. In certain circumstances, particularly where an applicant is of UK origin, a shorter period of residency may be accepted and a waiver granted by the appropriate vetting authority.

Criteria

0905. The criteria covering the requirement for DV clearance and the application of the criteria are contained in paras 0321 and 0322.

Responsibilities of Heads of Establishment

0906. Heads of establishments (HOE) are responsible for:

a. Assessing whether a post meets the criteria for being designated DV.

b. Ensuring that personnel are cleared to DV level before they are granted access to protectively marked information and assets to the levels specified in paras 0321 and 0322.

c. Keeping their DV posts under review and to a minimum and ensuring that only those which fully meet the criteria set out in paras 0321 and 0322 are retained.

d. Notifying the addition/deletion of a DV post or of a change in detail to:

Royal Navy	-	Within the RN to the appropriate CinC through the chain of command to the Naval Manning Agency; within MOD HQ and its outstations to the appropriate administrative authority.
Army	-	Hd Pers Sy(A)Sec, where necessary, through the chain of command and MOD (DISI/DI(IM)).
Royal Air Force	-	HQ PTC Sy 1 through command security staffs.
Other TLBs	-	PSyA.

e. Submitting annual returns of DV posts to the relevant PSyA when required to do so.

Emergency Unsupervised Access to TOP SECRET Information

0907. In exceptional circumstances an individual who is cleared to SC only may be given emergency unsupervised access to TOP SECRET information under the relevant Principal Security Adviser instructions. If required, DV clearance should be carried out as soon as possible. See also para 0326.

Those Ineligible for DV Clearance

0908. The following are **not normally** eligible for DV clearance:

a. Persons under 21 years of age (posts requiring DV clearance are not to be given to persons under 17 years of age).

b. Persons with less than 12 months' service.

c. Persons who have less than two years to serve.

d. Locally engaged civilians overseas.

0909. Where the above restrictions would cause special difficulties exceptional authority may be granted for DV clearance to be initiated in specific cases. If and when such authority is granted under the terms of sub-para 0908a, the requirements of para 0921 will apply. Requests for waivers of the above limitations should be sent to:

Royal Navy	-	DNSy ICP
Army	-	Pers Sy(A) Sec
Royal Air Force	-	HQ PTC Sy1
Other TLBs	-	DDefSy – Hd Pers Sy

Initiation of Clearance Action

Service Personnel

0910. The responsibility for initiating DV clearance is as follows:

a. **Before posting.** When DV is required for posting to a DV annotated appointment, the posting authority is responsible for initiating clearance action with the vetting authority for individuals who do not hold DV clearance and for individuals whose DV clearance will lapse within six months of the proposed date of appointment. Posting authorities are also to request the initiation/renewal of DV clearance whenever an individual is being considered for posting to a NATO appointment, to a diplomatic post or to an overseas DV appointment, irrespective of the subject's current clearance and/or lapse date.

b. **After posting.** Exceptionally, if an incumbent of a post requires DV clearance whilst in post, either because the clearance annotation of the post has been raised or to meet local requirements, the HOE concerned is responsible for initiating clearance action through the posting authority.

Civilian Staff

0911. The responsibility for initiating DV clearance is as follows:

a. **At recruitment.** If a post is to be filled by direct recruitment, employing establishments are to notify their civilian personnel management authority (CPMA) of the clearance requirement when the request for recruitment is made. The CPMA is then to submit a clearance request using the form at Annex 9A to the vetting authority. Establishments holding

delegated recruiting authority are to raise the request direct to the vetting authority using the same form on their own authority.

b. **Before posting.** Prior to a DV annotated post or appointment being filled by a staff transfer from one establishment to another or within an establishment, the CPMA is to check the subject's management file and consult the vetting authority to establish the subject's current level of clearance. If DV clearance action is required, the CPMA is to submit a request to the vetting authority in the form at Annex 9A.

c. **After posting.** If an individual requires DV after posting, eg through a reorganisation of duties, the HOE is responsible for initiating clearance action normally through the CPMA.

Clearance Action

0912. An initial assessment of the individual's suitability to undergo enquiries, based on available information, is made. If satisfactory, the individual is provided with a Security Questionnaire (MOD Form 1109), DV Supplement (MOD Form 1110) and Financial Questionnaire (MOD Form 1117) for completion and submission to the vetting authority. Cases are to be processed under the agreed administrative procedures for each Service Command and for each TLBs area of responsibility, ensuring that the confidentiality of the information provided by the individual is protected at all times.

0913. If, following the application for DV and before clearance is granted, circumstances arise which cast doubt on the reliability of the individual, the initiating authority or establishment must inform the vetting authority without delay.

Provisional DV Clearance

0914. Where it is essential for urgent operational or other exceptional reasons, the grant of a provisional DV clearance may be authorised by the vetting authority, before the full DV procedure has been completed. Such cases are to be kept to a minimum and the procedures associated with a SC clearance (para 0310) are to have been satisfactorily completed before a provisional clearance is granted.

0915. The full investigation is to be completed as soon as possible, so that the grant of the provisional clearance can be confirmed or otherwise.

Timescale

0916. A DV clearance involves extensive enquiries and may take up to six months to complete from receipt of the correctly completed security questionnaire, DV supplement and financial questionnaire at the vetting authority. It is important,

therefore, that requests for DV clearance are initiated as early as possible. When there is a need for urgent DV clearance to meet an operational need, advice should be sought from the vetting authority.

Notification

0917. The vetting authority will notify the initiating authority or establishment of the granting or denial of DV clearance. Where clearance has been granted to a member of staff, arrangements are to be made locally to inform the individual.

0918. If a DV cleared potential recruit is not employed, the clearance notification is to be retained until six months after the date of issue and is then to be destroyed.

Validity of Clearance

0919. DV clearance has replaced PV(TS) and EPV which in turn replaced PV clearance. Holders of PV(TS) and EPV clearances may be deemed to hold a valid DV clearance. A DV clearance will remain valid until resignation, retirement or the previously notified lapse date except where it is withdrawn or suspended or lapses when no longer required. It may require revalidating when an individual returns to duty after a period of absence of 12 months or more. See also para 0922.

Aftercare

0920. The personnel security process continues after a clearance has been granted. Aftercare arrangements are outlined in paras 1817 – 1825.

DV Review for Young People

0921. When a DV security clearance is granted to an individual who is under 21 years of age, a special annual review of the subject is carried out by the vetting authority. In addition, a supervisor has to be nominated by the subject's HOE and briefed to monitor the subject's character and conduct (see para 1821).

DV Review

0922. DV clearances will be reviewed at the intervals laid down in para 0323. Responsibility for initiating the review of a DV clearance where there is a continuing requirement for the clearance rests with:

Royal Navy	-	Posting authorities for RN personnel and DVA for civilian staff.

Army	-	DVA for Army personnel and civilian staff.
Royal Air Force	-	Station security staff.
Other TLBs	-	DVA

Procedure

0923. A DV review involves:

a. Providing the individual with a Security Questionnaire (Review) Guidance (MOD Form 1127) and then asking him to complete MOD Form 1109, DV Supplement (Review) (MOD Form 1112) and Financial Questionnaire (MOD Form 1117).

b. A check of departmental records.

c. A further NIS check and credit reference check.

d. A check with the Security Service, but **only if** there has been a change of partner or of step-parent since the initial clearance or last review, or if the partners' parents were not checked during the previous clearance.

e. A subject interview although in some straightforward cases this may be dispensed with.

f. Where further investigation is warranted, further interviews with supervisors and referees as necessary.

0924. Where employment in a DV post is unlikely to continue beyond a further short period (up to 12 months) an extension of the current clearance may be possible without recourse to formal review action. The circumstances should be made clear to the vetting authority and a short extension requested.

Review on Change of Personal Circumstances

0925. A DV clearance is to be revalidated if the subject marries, remarries or sets up a stable unmarried relationship living with someone as a couple or reports a change of co-residents. Personnel holding a DV clearance who report such a change in their circumstances are to be asked to complete a Change of Personal Circumstances Questionnaire (MOD Form 1126). Cases are to be processed under the agreed administrative procedures for each Service/TLB ensuring that the confidentiality of the information provided by the individual is protected at all times.

Dormant/Reserve/War Appointments

0926. Posting authorities have the task of ensuring that DV clearances for persons earmarked for such appointments remain valid

.

This page intentionally left blank.

ANNEX A

RESTRICTED – STAFF (When completed)

To: [Vetting authority] From:[Establishment]

Ref: [Establishment ref] Date:

REQUEST FOR DV CLEARANCE OF A CIVILIAN EMPLOYEE

1. DV clearance is requested for:

Surname……

Forenames……

Grade…… Present

Post/establishment……..

Correspondence

Address…….

Who is required for employment in a newly created post*/to replace*

Full name……..

Grade……

2. The post concerned is:

Establishment……

Post…….

3. Is indoctrination for access to CODEWORD, ATOMIC or IDO information required? If yes, please specify ……

4. Target date for completion……(If clearance is required within 4 months of the date of submission, a priority clearance is required and this form must be signed by an officer of Capt RN/Col/Gp Capt rank or Grade 7).

5. The following documents are enclosed*/will be forwarded*:

Personal File	[ ]	Staff Reports File	[ ]		
Medical File	[ ]	Discipline File	[ ]		
Unit Personal File	[ ]	5 Year Sick Absence Record	[ ]		

6. I certify that to the best of my knowledge the person nominated is suitable for DV clearance and that access will not be allowed until a certificate of clearance is received.

Signed……Name……(Block capitals)

Rank/grade……..…Tel no and ext……

RESTRICTED – STAFF (When completed)

This page intentionally left blank.

COMMERCIAL SECURITY GUARDS

This page intentionally left blank.

CHAPTER 10

COMMERCIAL SECURITY GUARDS

Introduction

1001. Full background concerning their employment is given in JSP 440 Volume 1, Chapter 18. Additional specialised information is contained in the Cabinet Office Manual of Protective Security, Chapter 3, Section 8. That chapter covers such matters as:

a. Suitability of firms.

b. Utilising List X procedures for certain contract guards.

c. Custody of STRAP material.

d. Conditions of contract.

Guidance on the appropriate level of clearance from BC to SC for contract personnel is given below.

Basic Check (BC)

1002. All contract guard force personnel must first be subjected to a BC. Details about this procedure are given in Chapter 11. Responsibility for undertaking the BC rests with the contractor, although this may be delegated to the sub-contractor. Within the MOD BC approval (see para 0502) authorises unsupervised access up to CONFIDENTIAL level to UK assets. For the rules relating to occasional access to SECRET, see para 1120. For the protection of unoccupied domestic sites or for the care and maintenance of surplus estate, a stand alone BC clearance is adequate. Only when a BC has been satisfactorily completed may an individual so cleared be put forward for vetting.

Counter Terrorist Check (CTC)

1003. After BC clearance, personnel who work at, or require access to, MOD sites in order to fulfil their responsibilities towards a commercial guarding contract are to be subjected to a CTC. This is done by requiring the individual to complete a security questionnaire (MOD Form 1109), which is then submitted to the respective vetting authority for action. Full details about the CTC procedure are contained in Chapter 6.

Security Check (SC)

1004. It is incumbent on HOEs to decide whether constant and frequent access **(see Note)** to information/assets marked above UK CONFIDENTIAL is required. Such access will be rare, therefore, the need for SC should be minimal. For personnel who are employed at certain highly sensitive locations, such as nuclear installations, SC will be required. For contract personnel who have unescorted access to weapons, ammunition or explosives eg as armourers or weapons storemen, see para 0610.

Vetting Lead Times

1005. As a guide, sponsors should allow at least six weeks for CTC or SC clearances in straightforward cases, eg where the subject has **no** Irish or foreign connections. Where there are such connections at least ten weeks should be allowed. This lead time is important since commercial guards are not permitted to start work at defence establishments until the necessary level of security clearance has been obtained. Any queries on vetting should be addressed in the first instance to the respective Principal Security Adviser.

Vetted Reserves

1006. To fulfil his commitments, a contractor should be required to maintain sufficient reserves of manpower who are security cleared to the requisite level. Normally, this will be in the ratio of 1:6 to the numbers employed on the contract.

Note: Personnel Security Notice S(PE) 95/9 refers

BASIC CHECK OF CONTRACTORS' EMPLOYEES

This page intentionally left blank.

CHAPTER 11

BASIC CHECK OF CONTRACTORS' EMPLOYEES

General

1101. Similar standards of reliability are expected of contractors' staff as for Service personnel and government employees. It should be made clear to contractors at an early stage that people employed on MOD work should meet a certain standard of reliability. In accordance with DEFCON 76, responsibility for initiating BC approval rests with the contractor however, security authorities are under remit to supervise the contractors' work in this field.

Level of Access

1102. The Basic Check is not a security clearance. However, confirmation that the BC has been carried out will provide sufficient assurance of reliability to allow contractors' employees frequent access, under normal supervision, to RESTRICTED and CONFIDENTIAL material of UK origin on a need-to-know basis.

1103. It should also be noted that a Security Check (SC) or Developed Vetting (DV) cannot be carried out unless a BC has been completed. Furthermore, the minimum level of clearance required to allow unescorted access to MOD Head Office sites is an SC.

Short Term Contractors

1104. In those cases where there is insufficient time before work is scheduled to start to subject contractors' employees to a Basic Check, arrangements are to be made with the relevant sponsor to have them properly escorted while on their premises. For contractors employed by the Armed Forces, see paras 1403 – 1404.

Verification of Identity

1105. An important part of establishing the reliability and integrity of contractors' employees is ensuring that they are who they say they are. Candidates must be asked to provide original documents to establish their bona fides. Duplicates and photocopies must not, under any circumstances, be accepted. Certified true copies of original documents are acceptable for onward transmission to MOD when necessary.

1106. The documents necessary to establish identity will vary according to the nationality of the individual concerned. Full details are given in Annex 5A.

Verification of Integrity

1107. The contractor must obtain two types of reference for an employee, each of which should cover at least the last three years. The first should, ideally, be obtained from the previous employer. Where this is not possible because the individual has been unemployed or his previous employer is no longer in business or declines to provide a reference on grounds of company policy, a second personal reference must be obtained. Where an individual has been in full time education a reference must be sought from the relevant school or other academic institution. In cases where the individual has served in the Armed Forces or in the Civil Service during the past three years, references should be sought from previous line managers named by the candidate and not from the Service or Department.

1108. The second type of reference must be sought from a personal referee nominated by the candidate. Ideally, such a referee should be of professional standing eg. solicitor, civil servant, teacher, accountant, bank manager, doctor or officer of the Armed Forces. However, individuals should be advised to nominate such a person only when their personal knowledge of that individual is likely to be sufficient to allow them to provide a considered reference. Where the individual is unable to nominate such a person, a reference should be obtained from personal acquaintances to whom they are not related, by birth or marriage, or involved in any financial arrangement with the candidate.

1109. Where an individual has been overseas for a period greater than six months during the past three years every effort must be made to obtain a reference from the overseas employer.

1110. To ensure that the right questions are addressed about the candidate's integrity and to minimise the workload on referees and hence increase the probability of obtaining a quick reply, references should be sought using the covering letter for the BC Reference Report Form at Annex A.

1111. Where necessary, references may be obtained by telephone, but they must be recorded on the standard form (Annex 5B1-2) together with identifying details of the referee and of the person obtaining the reference. The fact that the reference has been obtained by telephone must be recorded.

1112. For a current employee who has been with the company for the past three years or more a perusal of company records and a check with a manager, using the standard reference form, is sufficient and no further references are required.

Criminal Record Declaration

1113. Candidates must also make a self-declaration of any "unspent" criminal convictions that they may have, using the proforma at Annex C. (See Note). Individuals are not obliged to reveal the information on the Criminal Record Declaration proforma to the company. If they do not wish to do so, the proforma should be returned to the company in a sealed envelope which will be returned to the relevant vetting authority unopened. (See para 1116).

> **Note:** Under the provisions of the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 for persons on the mainland of Great Britain, and the Rehabilitation of Offenders Act 1978 (Exception) Order 1979 for persons in Northern Ireland, certain convictions are deemed to be 'spent' after a given period of time if the offender remains free of conviction during that period.

The Basic Check Verification Record (BCVR)

1114. Examination of the documents necessary to establish the subject's identity and nationality, obtaining the necessary references and the Criminal Record Declaration may be performed by either the MOD Sponsor or establishment security officer or, in the case of a List X company, the security controller. The details of the documents seen must be recorded on the BCVR at Annex 5B together with the details of those who actually made the checks. All the references must also be attached to the BCVR.

Approval of Access

1115. Providing the:

a. Necessary identification documentation has been recorded as being seen;

b. Appropriate references are attached and none of the referees has given any indication that he has reservations about the suitability of the candidate to be employed on sensitive MOD work;

c. Candidate is a British national (not a dual nationality);

d. Candidate has supplied a Criminal Record Declaration, not in a sealed envelope, showing no convictions or pending prosecutions;

e. Candidate has not worked, or resided overseas, for more than six months during the past three years; the MOD Sponsor, the company security controller or the ESyO may then grant approval for the candidate to have access to protectively marked material within the limits set out in para 1102. In the Central TLB, DPA and

Trading Funds for Non List X contractors, the MOD Sponsor or ESyO will forward a copy to all BC documentation along with the appropriate completed security questionnaire to the DVA for assessment and decision.

Approval by Principal Security Adviser

1116. If, however, any of the above conditions are not met, a copy of the BC documentation together with the Criminal Record Declaration must be forwarded to the respective PSyA with a covering letter explaining the reasons for referral. The originator should retain originals of the documentation (except the Criminal Record Declaration if submitted in a sealed envelope). After consideration, the relevant PSyA will advise the originator whether approval has been granted for the candidate to have the relevant access.

Counter Terrorist Check (CTC)

1117. When a contractors' employee is being submitted for a CTC, at the same time as a BC, there is no requirement to carry out a separate identity check or to seek a self declaration of criminal convictions as part of the BC since these also form a part of the CTC procedure.

Retention of Documentation

1118. The documentation associated with a BC should be retained by the MOD sponsor for a period of twelve months after the subject has ceased to be employed.

1119. Where an employee of a List X or Non List X company leaves to join another such company, the individual may have his BCVR with the accompanying documentation transferred to the new company together with a reference from the losing company.

Occasional Access to SECRET

1120. When List X and Non List X companies have staff who are only BC

approved, but who are required to have occasional, **intentional** access to UK SECRET material, they must complete:

a. In List X companies a Criminal Conviction Declaration form as shown at Annex D. This form must then be forwarded, in a sealed envelope, to the DVA, which will advise the company as soon as the Criminal Record Check against the NIS index has been completed.

b. In Non List X companies the Application for a NIS Check for a Civilian Employee as shown at Annex 5C and the Declaration thereto at Appendix 1. Annex 5C only must then be forwarded, in a sealed envelope, to the DVA, which will advise the MOD sponsor/ESyO as soon as the Criminal Record Check against the NIS index has been completed.

Competing for Quality (CFQ)

1121. For background see para 0339.

This page intentionally left blank.

ANNEX A

BASIC CHECK

Covering Letter for Reference Report Form

The draft covering letter shown below may be used together with the attached Basic Check Reference Report Form. Alternatively, companies may wish to include the Report Form with their normal letter requesting references.

Subject:_____

You may be aware that we are required to seek references to confirm the reliability of persons who may have access to certain classes of Government material. The person named above who is an employee of/has applied for employment with this company comes within the terms of this procedure. He/she has given us your name as a previous employer/personal acquaintance willing to give such a reference. It would be appreciated, therefore, if you would be good enough to let us have any information about him/her, which you think may help us in assessing his/her reliability, by completing the attached report form and returning it to us as soon as possible.

Your reply will be treated in the strictest of confidence.

Your co-operation and understanding in this matter will be greatly appreciated.

Yours sincerely

This page intentionally left blank.

ANNEX B

BASIC CHECK REFERENCE REPORT FORM

Subject:_____

1. Are you related to the subject? If so please state your relationship:

2. Over what period have you know the subject? Please give approximate month and year:

From: To:

3. Please state the nature and depth of your acquaintance:

4. Do you believe the subject to be strictly honest, conscientious and discreet?

5. Do you know of any factor concerning the subject which might cause his/her fitness for employment on sensitive work to be questioned? If so please give details. (Among relevant factors are significant financial difficulties, abuse of alcohol or drugs, an extravagant mode of living or signs of mental or physical illness which may impair judgement or reliability).

The above answers are correct to the best of my knowledge and belief.

Name: Signature:

Contact address and telephone:

Company Stamp (if applicable)

This page intentionally left blank.

ANNEX C

ACCESS TO GOVERNMENT OWNED MATERIAL

Criminal Record Declaration

The company named at the bottom of this form has Government contracts, some or all of which require it to hold material or information which is the property of the Government. The company has a duty to protect these assets while in its possession and this obligation extends to its employees and agents. Since you are, or may become, such a person please complete the following:

1. Surname: 2. Full forenames:

3. Date of Birth: 4. Full permanent address:

5. Have you ever been convicted or found guilty by a Court of any offence in any country (excluding parking but including all motoring offences even where a spot fine has been administered by the police) or have you ever been put on probation or absolutely/conditionally discharged or bound over after being charged with any offence or is there any action pending against you? You need not declare convictions which are "spent" under the Rehabilitation of Offenders Act (1974). **Yes/No***

If yes please give details here:

6. Have you ever been convicted by a Court Martial or sentenced to detention or dismissal whilst serving in the Armed Forces of the UK or any Commonwealth or foreign country? **Yes/No***

If yes please give details here:

7. Do you know of any other matter in your background which might cause your reliability or suitability to have access to government assets to be called into question? **Yes/No***

If yes please give details here:

I declare that the information I have given above is true and complete to the best of my knowledge and belief. I understand that any false information or omission in the information I have given may disqualify me for employment in connection with Government contracts.

Your signature: **Date:**

The information you have given will be treated in strict confidence. You do not need to show the completed form to any representative of the company. If you wish you may place the completed form in a sealed envelope, sign your name across the flap and return it to the company. The company will then forward it to the Government department concerned.

* Delete whichever is not appropriate

Name and address of sponsoring company:

This page intentionally left blank.

ANNEX D

RESTRICTED-STAFF (When completed)

CRIMINAL CONVICTION DECLARATION FORM (List X firms only)

Notes on completion:

1. Please use BLOCK CAPITALS in black ink or typescript, using an additional information page if necessary:

2. Answer all questions as fully as possible. Where the answer is not known, enter **N/K** or **N/A** where an answer is not applicable.

IMPORTANT: PLEASE READ THESE NOTES BEFORE COMPLETING THE FORM.

In the interests of national security, safeguarding Parliamentary democracy and maintaining the proper security of the Government's activities, it is the policy of HMG that no one should be employed in connection with work the nature of which is vital to the interests of the State;

(i) who is, or has previously been involved in, or associated with, espionage, terrorism, sabotage, or actions intended to overthrow or undermine Parliamentary democracy by political, industrial or violent means; (this includes membership of, or association with, any group which is involved with such activities).

(ii) who is susceptible to pressure or improper influence, for example, because of current or past conduct; has shown dishonesty or lack of integrity which throws doubt on their reliability; or has demonstrated behaviour, or is subject to circumstances which may otherwise indicate unreliability.

In accordance with this policy, all individuals in posts which require them to have access to MOD SECRET information and assets may be subject to a check against the National Collection of Criminal Records. When completing this form, you must declare any criminal convictions that you may have, including those which are "**spent"**. In accordance with the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975, and the Rehabilitation of Offenders (Northern Ireland) Order 1978 (Exceptions) Order 1979, spent convictions may also be taken into account where national security is concerned. In Northern Ireland spent convictions may also be taken into account where the protection of public safety or public order is involved. The relevance of particular criminal offences is a matter for the Department to decide; **YOU MUST THEREFORE DECLARE ALL CONVICTIONS INCLUDING THOSE WHICH INVOLVED A JUVENILE COURT, WHETHER OR NOT "SPENT" UNDER THE ABOVE ACTS. THERE ARE NO EXCEPTIONS.**

Once completed, this Form should be placed in a sealed envelope, with your signature over the flap, and handed to the Security/Personnel Officer for onward transmission to the Ministry of Defence.

CURRENT SURNAME:.....…

ANY OTHER SURNAME USED:.....…

FULL FORENAME(S):.....….

DATE OF BIRTH:...../...../.....PLACE OF BIRTH:.....……..

CURRENT NATIONALITY (including any dual nationality):.....

PROOF OF BRITISH CITIZENSHIP (if applicable):.....

PROPOSED EMPLOYMENT:.....…

RESTRICTED-STAFF (When completed)

RESTRICTED-STAFF (When completed)

FINAL DESTINATION:

DVA – Building 107, Imphal Barracks'

Fulford Road, YORK YO1 4AU

Please supply your addresses for the past five years:

	From	To
1.		
2.		
3.		

Have you ever been convicted by a Court, including a Juvenile Court, of any offence in any country (excluding minor motoring offences?

YES	NO

If you have answered YES please give details of the offences referred to:

Nature Of Offence	Sentence Awarded	Date Sentence Awarded

Have you ever been convicted by Courts Martial or sentenced to dismissal whilst serving in the Armed Forces of the UK or any other Commonwealth or foreign country.

YES	NO

If you have answered YES please give the following details:

Service (RN/ARMY/RAF)	Rank and Serial Number	Nature of Offence	Sentence(s) Awarded

RESTRICTED-STAFF (When completed)

RESTRICTED-STAFF (When completed)

DECLARATION: I declare that I have read and understand Her Majesty's Government's policy concerning individuals employed in work, the nature of which is vital to the interests of the State, as described on page one. I understand that this Form will be submitted for checking against the records in accordance with that policy.

I declare that the information I have given is true and complete to the best of my knowledge and belief. In addition, I understand that any false statement or deliberate omission in the information I have given on this Form may disqualify me for employment in connection with Crown contracts.

SIGNED.....DATE.....

COMPANY ADDRESS

FOR NOTIFICATION

OF DECISION:

RESTRICTED-STAFF (When completed)

This page intentionally left blank

SECURITY CHECK OF CONTRACTORS' EMPLOYEES

This page intentionally left blank

CHAPTER 12

SECURITY CHECK OF CONTRACTORS' EMPLOYEES

Purpose and Procedures

1201. The purpose of the Security Check (SC) and the procedures for carrying out SC clearances are set out in paras 0310 and 0311.

Vetting Authorities

1202. The DVA is responsible for granting SC clearances to contractors' employees including Non List X company employees working on single Service (including US Forces) contracts and on tri-Service contracts with a single Service lead.

1203. The DVA is similarly responsible for vetting Non List X company employees working in or covered by:

a. MOD Head Office sites.

b. Contracts placed by the Defence Procurement Agency (DPA).

c. Directorate of Works Services (excluding DWS(USF) employees at US Forces locations).

d. MOD contracts

e. Nuclear and other DPA establishments.

Responsibility for List X Employees

1204. This is divided as below:

a. Service Command/TLBs are responsible for sponsoring clearances for List X contractors on Service sites

b. List X Security Controllers apply direct to the DVA for clearances for such staff operating on all List X sites.

Nationality

1205. The nationality rules governing eligibility for employment within MOD are contained in Chapter 4.

Residency

1206. Candidates for SC clearance, regardless of origin, should normally have resided continuously in the UK immediately prior to their application for a minimum of five years. In certain circumstances, particularly where an applicant is of UK origin, a shorter period of residence may be accepted, subject to a waiver being granted by the appropriate vetting authority. See also para 0804.

Criteria

1207. The criteria covering the requirement for SC clearance and the application of the criteria are contained in paras 0313 and 0314.

1208. In the case of all MOD Head Office sites, the minimum level of clearance required to allow unescorted access is an SC clearance. In all other MOD establishments, Defence Agencies and GOCO sites, the minimum level of clearance is determined in accordance with the level of access required. For commercial security guards, see Chapter 10.

Restrictions – Young Persons

1209. Personnel under 21 years of age may be granted SC clearance. However, whilst under 17 years of age they should not normally be allowed access above CONFIDENTIAL.

Timescale

1210. SC clearance will normally take between four to six weeks to complete, from the date of receipt of the correctly completed security questionnaire at the vetting authority, but it can take longer.

Authorization

1211. The vetting authority will inform the security controller for List X company employees, or the project manager or establishment security officer (ESyO) for Non List X company employees when clearance has been authorised. The latter are responsible for notifying the contractor.

1212. Contractors' employees must not be engaged on MOD contracts until the appropriate clearance is received.

Access Control

1213. In all cases where it is not possible to give approval for SC clearance to an individual, the security controller, or project manager or ESyO is to ensure that the necessary access control is enforced.

Validity

1214. An SC clearance is valid for a maximum period of three years from the date of issue except in the case of:

a. Employees of List X companies (see para 1220).

b. Notification that a clearance has been withdrawn, suspended or lapsed.

c. Cessation of employment when SC clearance may be lapsed, in which case transfer/reactivation of the previous SC clearance by the receiving authority within 12 months may be acceptable providing no change of circumstances has arisen.

SC Clearance and Review of Non List X Company Employees

Initial Clearance Action

1215. SC clearance action is to be initiated by the project manager or ESyO with the individual being asked to complete a Security Questionnaire (MOD Form 1109). SC clearance may be sought concurrently with the BC but a clearance cannot be granted until the vetting authority has received confirmation that the BC has been satisfactorily completed.

SC Review

1216. If required, SC clearances will be renewed every five years. Responsibility for initiating the review of an SC clearance rests with the MOD sponsor, project manager, ESyO or (RAF only) station security officer. The individual is to be provided with a Security Questionnaire (Review) Guide (MOD Form 1127) and be asked to update his personal details by completing a Security Questionnaire (MOD Form 1109).

Review on Change of Personal Circumstances

1217. An SC clearance is to be revalidated if the subject marries, remarries or sets up a stable unmarried relationship living with someone as a couple, or reports a change of co-residents. Personnel holding an SC clearance who report such a change in their circumstances are to be asked by the project manager or ESyO to complete a Change of Personal Circumstances Questionnaire (MOD Form 1126) which should clearly state what the change of circumstance is.

Administrative Procedures

1218. Cases under paras 1215 to 1217 are to be processed under the agreed administrative procedures ensuring that the confidentiality of the information provided by the individual is protected at all times.

SC Clearance and Review of List X Company Employees

Initial Clearance Action

1219. SC vetting of List X company employees and their sub-contractors is undertaken by the DVA. The security controller of the company is to ask the individual to complete a Security Questionnaire (MOD Form 1109). SC clearance may be sought concurrently with the BC but access to protectively marked material cannot be granted until confirmation has been received that the SC has been satisfactorily completed.

SC Review

1220. The SC clearances for direct employees of a List X firm are reviewed every ten years whilst sub-contractors' clearances are reviewed every five years. The individual is to be provided with a Security Questionnaire (Review) Guide (MOD Form 1127) and be asked to update his personal details by completing a Security Questionnaire (MOD Form 1109).

Review on Change in Personal Circumstances

1221. An SC clearance is to be revalidated if the subject marries, remarries or sets up a stable unmarried relationship living with someone as a couple, or reports a change of co-residents. Personnel holding an SC clearance who report such a change in their circumstances are to be asked by the security controller to complete a Change of Personal Circumstances Questionnaire (MOD Form 1126) which should clearly state what the change of circumstance is.

Administrative Procedures

1222. Cases under para 1219 to 1221 are to be processed under the agreed administrative procedures ensuring that the confidentiality of the information provided by the individual is protected at all times. However, those uncleared List X company employees who require an SC clearance to work on MOD premises are to be cleared as for Non List X employees. See paras 1215 and 1216.

Confirmation of Clearance and Status

1223. Confirmation of clearances for List X company employees can be obtained from the security controller at each firm. Confirmation of the current List X status of a firm can be obtained from D Def Sy Info Sy(Industry).

Sponsorship for Overseas Visits: Non List X Employees

1224. Where such an employee requires security clearance to visit an overseas Government office or contractor, and where there is no relevant MOD sponsor or project manager, the personnel section of the Non List X company should fulfil the sponsorship role which will include the associated Basic Check verifications.

Potential List X Employees: Acceptance of Overseas Security Clearances

1225. Guidance is given in Annex A.

This page intentionally left blank.

ANNEX A

POTENTIAL LIST X EMPLOYEES: ACCEPTANCE OF OVERSEAS SECURITY CLEARANCES

1. It is generally accepted throughout the NATO area that, under the principle of reciprocity, a personnel security clearance issued by an individual's parent PSyA is accepted by another member nation for access to its classified material at the appropriate level, and where there is a need to know.

2. This usually arises in the following circumstances:

   a. Where a company in a NATO member country has received a classified contract from another member nation and its cleared employees require access to the material.

   b. Where there is a need for an individual from one NATO country to visit another in order to discuss or to access classified information on a specific subject.

3. As a result of the increased movement of the international labour force particularly between member states of the European Union (EU), a third scenario has become more common. UK firms are beginning to advertise their vacancies throughout the EU for specialists such as graduate engineers etc.

4. It has therefore been agreed that when a potential candidate for a List X company is identified but s/he is resident outside the UK, D DefSy InfoSy(IVCO) will ask the appropriate overseas security authority to grant the individual a security clearance to SECRET level. This can only be achieved for NATO member nations or for countries with which the UK has a General Security Arrangement (GSA). For other countries the SC application should be submitted in the normal way.

5. When a security clearance has been granted by the overseas security authority an equivalent level UK clearance should be issued. This will be valid for three years and be subject to the usual limitations regarding access to caveat material or to other foreign material. After three years, the DVA will effect re-vetting if it is still required.

This page intentionally left blank.

DEVELOPED VETTING OF CONTRACTORS' EMPLOYEES

This page intentionally left blank.

CHAPTER 13

DEVELOPED VETTING OF CONTRACTORS' EMPLOYEES

Purpose and Procedures

1301. The purpose of Developed Vetting (DV) and the procedures for carrying out DV clearances are set out in para 0319 and 0320.

Vetting Authorities

1302. The DVA is the vetting authority responsible for granting DV clearances to contractors' employees. It is responsible for carrying out the vetting for Non List X company employees working on single Service contracts (including US Forces) and on tri-Service contracts with a single Service lead.

1303. The DVA is similarly responsible for vetting Non List X company employees working in or covered by:

a. MOD Head Office sites.

b. Contracts placed by the Defence Procurement Agency (DPA).

c. Directorate of Works Services (excluding DWS(USF) employees at US Forces locations).

d. MOD contracts

e. Nuclear and other DPA establishments.

f. List X companies.

Nationality

1304. The nationality rules governing eligibility for employment within MOD are contained in Chapter 4.

Residency

1305. Candidates for DV clearance, regardless of origin, should normally have resided continuously in the UK immediately prior to their application for a minimum of ten years. In certain circumstances, particularly where an applicant is of UK origin, a shorter period of residence may be accepted and a waiver granted by the appropriate vetting authority. See also para 0904.

Criteria

1306. The criteria covering the requirement for DV clearance and the application of the criteria are contained in paras 0321 and 0322.

Designation of Posts

1307. It is the responsibility of the MOD sponsor or project manager to determine whether a post occupied by a contractor's employee meets the criteria for DV clearance.

Review of Posts by MOD Sponsor

1308. The MOD sponsor should keep DV posts occupied by contractors' employees under review, at least annually, to ensure that only those which fully meet the criteria set out in para 0321 are retained. DV posts relate to specific contracts only and it is the responsibility of the MOD sponsor to notify the vetting authority when the contract is either completed or an individual has left a project.

Annual Review of Posts by Principal Security Adviser

1309. The relevant PSyA will annually review all DV posts held by contractors' employees.

Those Ineligible for DV Clearance

1310. The following are not normally eligible for DV clearance:

a. Persons under 21 years of age.

b. Contractors' employees working on contracts which have less than 12 months to run.

Timescale

1311. DV clearance involves extensive enquiries which can take up to six months to complete. It is, therefore, important that requests for DV clearance are submitted well in advance of the commencement of a contract.

Notification of Clearance

1312. The DV clearance decision will be notified to the security controller, MOD sponsor or establishment security officer (ESyO) in writing. It will be their responsibility to inform the individual of the decision.

Validity

1313. A DV clearance is valid for a maximum period of five years from the date of issue except in the case of:

a. Employees of List X companies (see para 1319).

b. Notification that a clearance has been withdrawn, suspended or lapsed.

c. Cessation of employment.

DV Clearance and Review of Non List X Company Employees

Initial Clearance Action

1314. DV clearance action is to be initiated by the project manager or ESyO who is to confirm, in writing, to the vetting authority, the requirement for DV clearance. If initial enquiries are satisfactory, the individual is provided with a Security Questionnaire (MOD Form 1109), DV Supplement (MOD Form 1110) and Financial Questionnaire (MOD Form 1117) for completion and submission to the vetting authority.

DV Review

1315. If required, DV clearances will be renewed initially after five years and then every seven years. Responsibility for initiating the review of a DV clearance where there is a continuing requirement for the clearance rests with the vetting authority or, RAF only, station security officer. The individual is to be provided with a Security Questionnaire (Review) Guide (MOD Form 1127) and be asked to complete a Security Questionnaire (MOD Form 1109), DV Supplement (Review) (MOD Form 1112) and Financial Questionnaire (MOD Form 1117).

Review on Change of Personal Circumstances

1316. DV clearance is to be revalidated if the subject marries, remarries or sets up a stable unmarried relationship living with someone as a couple, or reports a change of co-residents. Personnel holding a DV clearance who report such a change in their circumstances are to be asked by the project manager or ESyO to complete a Change of Personal Circumstances Questionnaire (MOD Form 1126).

Administrative Procedures

1317. Cases under paras 1314 to 1316 are to be processed under the agreed administrative procedures for each Service's or TLB's area of responsibility, ensuring that the confidentiality of the information provided by the individual is protected at all times.

Security Appraisal Forms (SAFs)

1318. As a rule, SAFs are not issued in respect of Non List X company employees.

DV Clearance and Review of List X Company Employees

Initial Clearance Action

1319. The DV clearance of List X company employees is undertaken by the DVA. Action is initiated by the security controller of the company who is to confirm, in writing, to the DVA, the requirement for DV clearance. If initial enquiries are satisfactory, the DVA will forward, to the security controller, a Security Questionnaire (MOD Form 1109), DV Supplement (MOD Form 1110) and Financial Questionnaire (MOD Form 1117) for completion by the individual and return.

DV Review

1320. To ensure that DV clearances do not become outdated and to reflect the need for regular review, List X company employees' clearances will be reviewed initially after five years and then at least every seven years. The individual is to be provided with a Security Questionnaire (Review) Guide (MOD Form 1127) and be asked to complete a Security Questionnaire (MOD Form 1109), DV Supplement (Review) (MOD Form 1112) and Financial Questionnaire (MOD Form 1117).

Review on Change of Personal Circumstances.

1321. DV clearance is to be revalidated if the subject marries, remarries or sets up a stable unmarried relationship living with someone as a couple, or reports a change of co-residents. Personnel holding a DV clearance who report such a change in their circumstances are to be asked by the security controller to complete a Change of Personal Circumstances Questionnaire (MOD Form 1126).

Administrative Procedures

1322. Cases under paras 1318 to 1320 are to be processed under the agreed administrative procedures, ensuring that the confidentiality of the information provided by the individual is protected at all times.

Confirmation of Clearance and Status

1323. Confirmation of clearances for List X company employees can be obtained from the security controller at each firm. Confirmation of the current List X status of a firm can be obtained from D Def Sy

Security Appraisal Forms (SAFs)

1324. As a rule, SAFs are not issued in respect of List X company employees.

This page intentionally left blank.

SHORT TERM CONTRACTORS EMPLOYED BY THE ARMED FORCES

This page intentionally left blank.

CHAPTER 14

SHORT TERM CONTRACTORS EMPLOYED BY THE ARMED FORCES

Introduction

1401. The security measures to be enforced in respect of short term contractors differ considerably from those governing List X and other long term contractors. Both latter categories have an MOD sponsor. The rules governing security clearances for such contractors are given in Chapters 11, 12 and 13.

1402. All the Services engage contractors whose staff undertake short term work. This, in the context of security, is taken to be that scheduled to last 14 days or less. While security considerations must be paramount, the level of vetting or access control required must be assessed in the context of risk management. The outcome of the exercise will necessarily relate primarily to the latest threat assessment about an establishment's vulnerability and extend to:

a. The anticipated time frame for the work in hand; and

b. The commercial considerations on which contract work is based.

Overall, the object is to produce minimum disruption to normal site activities commensurate with good security practice.

The Basic Check

1403. The full background to this subject is given in Chapter 5.

1404. If the time factor permits, all short term contractors' employees should be subjected to the Basic Check. This is because virtually all Service establishments contain RESTRICTED assets which such persons will inevitably see or access. On occasions, however, the time available before the contractor has to start work will be so short as to permit only the application of access control measures and, where possible, escorting. See para 1412.

Verification of Identity

1405. Full particulars are shown in Annex 5A where the requirements are specifically stated. Responsibility for establishing identity rests with the main

contractor, who may delegate this task to a sub contractor. The establishment security officer (ESyO) has responsibility to make sure that the contractors/sub contractors are verifying identity conscientiously.

Counter Terrorist Checks

1406. The full background to this subject is given in Chapter 6 with paras 0608 and 0612 to 0614 being particularly relevant.

Contractors' Staff

1407. Those needing entry to Service establishments will normally be required to complete a Security Questionnaire (MOD Form 1109) on which the CTC box at page 1 has first been ticked by the firm's respresentative or the ESyO.

1408. Once MOD Form 1109 has been filled in by the individual the firm's representative will complete page 12 and record which documents (Annex 5A) have been used to establish the subject's identity.

CTC Processing

1409. Only in those cases where either of the following are revealed is full CTC processing required.

a. Close Irish (see Annex 6A for details) or

b. Specific overseas connections (see Annex 6B)

Access Control Measures

1410. For all cases not covered by paras 1407 or 1409, the particulars on MOD Form 1109 are to be used as the basis for filling in a pass which is to be issued under local arrangements authorising an individual access to a Service establishment.

Extended Basic Checks

1411. In rare instances it may be necessary to establish more about an individual's suitability for a post. This may be done by extending the BC to include:

a. Referral to the National Identification Service (NIS) for a criminal records check and/or

b. Completion and processing of a Financial Questionnaire.

Access Controls

1412. This subject has a close relationship with, but is **not** an integral part of, vetting. This arises because those persons who are not security cleared for access to Service establishments need to be controlled through such means as official passes, photographs, booking in and out and escorts. Some guidance on these matters may be found in Chapter 6, paras 0612 to 0614. Further material is given in JSP 440 Volume 1, Chapter 5, Section IX.

This page intentionally left blank.

CHAPTER 15

(SPARE)

This page intentionally left blank

CHAPTER 16

(SPARE)

This page intentionally left blank

DENIAL, WITHDRAWAL, SUSPENSION AND LAPSING OF SECURITY CLEARANCE

This page intentionally left blank.

CHAPTER 17

DENIAL, WITHDRAWAL, SUSPENSION AND LAPSING OF SECURITY CLEARANCE

Introduction

1701. The decision to deny or withdraw security clearance from Service personnel, civilian staff and contractors' employees is made by the relevant authority (see Chapter 2) who ensures that factors outside the field of security, particularly career interests, are taken fully into account. The decision to deny or withdraw a security clearance is always made in accordance with the guidance in the Cabinet Office publication, 'Manual of Protective Security – Personnel Security', Chapter 4 of March 1998 and with the relevant internal procedures for appeals against adverse security vetting decisions. See para 1709 et seq.

Definitions

Denial

1702. Denial of security clearance is the refusal to grant a clearance.

Withdrawal

1703. Withdrawal of a security clearance is the removal of a clearance previously granted.

Suspension

1704. Suspension of security clearance is the temporary removal of a clearance pending an investigation and/or administrative action.

Lapsing

1705. Lapsing of a security clearance occurs when a clearance has exceeded its period of validity or when the security authorities, in conjunction with personnel/civilian management, consider that the holder no longer requires that clearance to conduct his duties.

Consequential Effect of Denial or Withdrawal of DV Clearance

1706. The denial or withdrawal of Developed Vetting (DV) clearance does not necessarily imply withdrawal or disqualification of Security Check clearance. Any consequential effect on SC clearance is notified at the time. Thus, the decision to allow an individual to retain SC clearance after denial or withdrawal of DV clearance is deliberate and indicates that he has been assessed and confirmed as suitable for filling an SC post.

Notifying the Individual

1707. Wherever possible, individuals should be informed of the outcome of vetting enquiries. See para 0327 for the position at recruitment. They should also be given early notice of factors likely to call into question their suitability to retain security clearance as well as the opportunity to challenge adverse information or conclusions.

1708. Where there are clear grounds for supposing that security clearance will be denied or withdrawn, the facts of the case should be agreed as far as is possible with the subject before a final decision on clearance is taken. This will include agreeing a factual record of any subject interview. This does not apply if the clearance is an integral part of the initial recruitment process. Any interviews will be conducted after consideration of source protection and under the umbrella of vetting confidentiality.

Appeals Procedures

1709. The internal appeals procedures against adverse security vetting decisions for Service personnel, civil servants and employees of MOD contractors are at Annexes A, B and C. These are not, however, available to recruits. Individuals who have exhausted these procedures and remain dissatisfied with the result may, where the decision to deny or withdraw a clearance, submit an appeal to the independent Security Vetting Appeals Panel. The Secretariat function for the Panel will be carried out by the Security Division of the Cabinet Office who will provide guidance notes for appellants.

Administrative Procedures

1710. The decision to deny or withdraw a security clearance will be notified by the security authorities to the appropriate personnel/civilian management branch and the head of establishment (HOE). The notification will state whether and when the decision may be reviewed.

1711. On receipt of the decision to deny or withdraw a security clearance, the relevant personnel/civilian management branch and HOE are to amend the personal security records as necessary.

1712. When the HOE is informed of a decision to deny or withdraw a security clearance he may be given specific instructions on action to be taken.

Retrospective Denial/Withdrawal of Security Clearance

1713. When a person is dismissed/discharged from the Armed Forces or Civil Service before the decision to deny or to withdraw a security clearance has been made, the normal rule for reporting such a fact to the Security Service is to be followed. Similarly, every effort is to be made to inform the individual where security clearance has been denied/withdrawn.

1714. Spare

Decisions Affecting Contractors

1715. Where a security clearance cannot be granted or is withdrawn, the Principal Security Adviser will notify the sponsor/project manager. It will be the responsibility of the latter to ensure that the decision is enforced. If the decision is likely to be difficult for the contractor to implement, he should consult the security authorities.

Suspension/Restoration of Security Clearance

1716. The decision to suspend a security clearance will be notified by the Principal Security Adviser to the individual's HOE. A copy of this notification will be sent to the appropriate personnel/civilian management branch. If the concerns that gave rise to the suspension of clearance are allayed and it is decided to restore the suspended clearance, the Principal Security Adviser will notify the subject's HOE accordingly.

1717. Suspension of a security clearance is a temporary measure pending the collation of information that will enable the security authorities to make a decision on whether to reinstate or withdraw a clearance. Suspension is to be kept under review. It can relate either to SC, DV or both. In the event of restoration of a clearance, the terms of that restoration and its relationship to any other clearance is to be specific.

Review of Previously Adverse Cases

1718. Where, on denial or withdrawal of security clearance, the decision is stated to be subject to review after a given period, the case may be reconsidered at any time after the expiration of that period, providing the need for clearance remains and the individual is considered by his HOE to be suitable.

This page intentionally left blank.

ANNEX A

APPEALS AGAINST ADVERSE SECURITY VETTING DECISIONS: INTERNAL PROCEDURES FOR SERVICE PERSONNEL

Naval Service

1. If a security clearance is recommended to be denied or withdrawn, the recommendation is to be put to the Chief of Staff to 2SL/CNH. Prior to the recommendation being reviewed, a subject interview will be conducted and the individual will sign to acknowledge that the facts in the interview report are a true reflection of the interview. If the recommendation is upheld, RN personnel may immediately state a complaint under the normal redress procedures provided for in the Naval Discipline Act 1957. The Admiralty Interview Board will consider the complaint and the individual will be informed of its decision.

Army

2. If a security clearance is to be denied or withdrawn, the individual will either be informed personally by his Commanding Officer or by the Head of Personnel Security (Army) Secretariat at an interview. Whenever feasible and appropriate, the Head of Personnel Security (Army) Secretariat will conduct an interview in those cases involving denial or withdrawal of a high level of security clearance and in instances where a career implication is involved. The background leading to the decision and the right to make a redress of complaint will be explained at the interview. If individuals are not satisfied with the outcome, they may appeal to their Commanding Officer under the normal redress of complaint procedures provided for in the Army Act 1955. The redress of complaint may be considered by the Army Board under these procedures. The individual will be informed of the Army Board's decision.

Royal Air Force

3. If a security clearance is to be denied or withdrawn, the individual will be interviewed under arrangements made by GC Prov & Pers Sy(RAF). An appeal can be lodged with the relevant Personnel Security Panel and may proceed to the Air Force Board. In addition, the appellant may follow the normal redress of grievance procedure provided for in the Air Force Act 1955. If, having lost an appeal against a vetting decision, an individual's redress application reaches the Air Force Board, the redress will be considered by Board members who were not involved in staffing the vetting appeal. The individual will be informed of the Air Force Board's decision.

Footnote: The existence of the Security Vetting Appeals Panel shall be drawn to the attention of individuals at the time they are informed of the arrangements for their internal appeals procedures.

ANNEX B

APPEALS AGAINST ADVERSE SECURITY VETTING DECISIONS: INTERNAL PROCEDURES FOR MOD CIVIL SERVANTS

Action Prior to an Appeal

1. Upon a clear indication that a clearance is to be denied or withdrawn and with a reasonable expectation (after consultation with the Personnel Management Authority) that an employee's career will be affected, the individual is to be invited to attend for interview with a Defence Vetting Agency (DVA) assessor and provided with a copy of the evidence (or reasons as far as is possible) on which any future action will be based.* The subject is then to be given a set period of time to correct any area which he or she does not consider to be a true record and be allowed to comment on their situation generally. Following such action, the DVA assessor will decide either:

a. to grant or to continue clearance, with appropriate aftercare as necessary; or

b. to recommend that clearance should be denied or withdrawn.

2. In the event of the assessor's recommendation being that clearance should be denied or withdrawn, the case is to be referred to the Service Command/D Def Sy for a decision on whether:

a. to grant or to continue clearance, with appropriate aftercare as necessary; or

b. to deny or withdraw clearance.

*A copy of this procedure shall be made available to potential appellants at the interview with the DVA assessor when the existence of the Security Vetting Appeals Panel shall also be drawn to their attention.

The Appeal

3. In the event of clearance being denied or withdrawn, the individual is to be so informed (with the reasons for the decision being stated as far as is possible) and given 28 days in which to submit a written appeal to PUS. The appeal is to be forwarded direct to the relevant personnel security staff for review and, unless the original decision is reversed, staffing to PUS or to his nominated deputy for a ruling on whether the original decision to deny or withdraw should stand. The appellant may opt for the appeal to be heard orally and may be accompanied by a colleague or by a representative of a recognised Trade Union at the hearing. The individual

should be informed of the outcome of the appeal, with the reasons for the decision being stated as fully as possible.

ANNEX C

APPEALS AGAINST ADVERSE SECURITY VETTING DECISIONS: INTERNAL PROCEDURES FOR MOD CONTRACTORS' EMPLOYEES

Action prior to an Appeal

1. Upon a clear indication that a clearance is to be denied or withdrawn, the Defence Vetting Agency (DVA) assessor will provide the individual with a copy of the evidence (or reasons as far as is possible) on which any future action will be based. This will usually be done in writing, but there may be occasions when an interview with a member of the Agency's staff is appropriate.* The subject is then to be given a set period of time to correct any area which he or she does not consider to be a true record and be allowed to comment on their situation generally. Following such action, the DVA assessor will decide either:

a. to grant or to continue clearance, with appropriate aftercare as necessary; or

b. to deny or withdraw clearance.

The Appeal

2. In the event of clearance being denied or withdrawn, the individual is to be so informed (with the reasons for the decision being stated as far as is possible) and given 28 days in which to submit a written appeal. The appeal is to be forwarded direct to the Chief Executive of the DVA for review of all the circumstances, and for a ruling on whether the original decision to deny or withdraw should stand. In exceptional or finely balanced cases, the Chief Executive DVA may elect to refer the matter to the relevant personnel security staff for consideration, including possible referral to PUS or to his nominated deputy. The individual should be informed of the outcome of the appeal, with the reasons for the decision being stated as fully as possible.

* A copy of this procedure shall be made available to potential appellants when writing to/interviewing them prior to an appeal when the existence of the Security Vetting Appeals Panel shall also be drawn to their attention.

This page intentionally left blank.

PERSONNEL SECURITY RESPONSIBILITIES OF HEADS OF ESTABLISHMENTS

CHAPTER 18

PERSONNEL SECURITY RESPONSIBILITIES OF HEADS OF ESTABLISHMENTS

Background

1801. Vetting is a process for establishing the suitability of personnel for access to protectively marked or sensitive assets and for ensuring that those who are granted such access remain suitable. Given that vetting does not provide a definitive and constant level of total assurance it is incumbent on HOEs, a definition of which is given at para 11b in the Introduction to this Volume, to take a positive interest in those under their control. This chapter sets out the need for active, yet properly balanced, supervision throughout the chain of command and line management.

The Head of Establishment (HOE)

1802. Keeping personnel security under review is a continuous process. HOEs and their subordinates play a very important role in ensuring the security of their organisation, particularly in respect of personnel security. Except for personal friends and close colleagues, an individual's superior officer is likely to have a more detailed and accurate knowledge of him/her than anyone else in the organisation.

1803. It is particularly noteworthy in that in many recent espionage cases, both in the UK and overseas, superior officers had been aware to some extent that a security problem had arisen but had failed to appreciate its significance or had not realised their responsibility for reporting the matter.

Responsibilities of Heads of Establishments

1804. In respect of their staff, HOEs are responsible for:

a. Setting the requisite security clearance levels, if any, of posts in consultation with their Establishment Security Officer (ESyO).

b. Briefing them on the security aspects of their job and on the level of security performance expected of them.

c. Monitoring their behaviour and, where relevant, reporting on their security performance.

d. Creating a positive climate in which security is given an appropriate priority and individuals are encouraged to discuss concerns before they become security problems.

e. Dealing with problems and discussing any concerns with their ESyO.

1805. Apart from the wider responsibilities listed at para 1804 above, HOEs are also responsible for the following, guidance on which is given in paras 1816 to 1825 below.

a. Security education and awareness training.

b. Aftercare including Incident Reporting and annual security appraisals.

c. Monitoring contacts by their staff with CSSRA.

d. Ensuring that a vetting register is maintained.

Setting Clearance Levels

1806. It is usually the responsibility of HOEs in consultation with the ESyO to decide the vetting requirements for particular posts and to review those requirements at suitable intervals. Individuals should be security cleared to a level consistent with the access they need to protectively marked assets. Over categorisation of posts is both a waste of staff resources and money. The responsibility of HOEs towards DV posts is detailed at para 0906.

Briefing

1807. The HOE is also responsible for briefing staff on arrival or on change of job about any aspects of the work that might raise issues of security or potential conflicts of interest. Similarly, they may be involved in the briefing of individuals before they are granted access to particularly sensitive assets.

Monitoring Staff

1808. The vast majority of staff are security cleared without difficulty and throughout their service never give cause for concern. However, the MOD is reliant on HOEs and their subordinates to spot potential difficulties and draw attention to them.

1809. HOEs and their subordinates are expected to monitor the behaviour of their staff for security. They should look out for the types of behaviour described in

Annex A which could suggest that a member of staff is unreliable or susceptible to adverse pressure. Particular attention should be paid to persons under 21 years old whose character will still be forming. Guidance for line managers and supervisors of personnel aged under 21 occupying DV posts is given in Annex B.

1810. In monitoring the behaviour of staff, it is very important that a sense of perspective is maintained. It is not the intention that HOEs or superiors should take

an unnecessarily close interest in individuals or adopt a censorious approach to their personal lives.

Creating a Positive Security Climate

1811. It is unusual for serious security problems to arise with personnel who feel able to express themselves freely and are able to approach a superior about problems. HOEs should create an atmosphere in which those who work for them can feel confident that there will always be a sympathetic ear to any matter that they consider might have a bearing on security. It should be emphasised that such matters will be treated in confidence and discussed, if necessary, only with the ESyO or his staff.

Dealing with Problems

1812. When a person has expressed any level of concern about a security matter, the HOE will need to decide whether it is of security significance. Where the information is not of serious concern, reassurance and advice should be offered. However, where it appears to be serious or its significance is unclear, the ESyO should be consulted before any further action is taken.

1813. Should a HOE receive security allegations about an individual or about someone elsewhere in government service, regardless of their position, it should be reported to the ESyO unless it is clear that the story is ill-founded or malicious. The ESyO will not assume that any allegation is true without taking steps to verify what has been reported or seeking advice. The generic responsibilities of the ESyO are shown at JSP 440, Volume 1, Chapter 2 para 0227 – 0228.

1814. It is important that all allegations of a security nature are resolved for the sake of all concerned. Any lingering doubts or suspicions are likely to demoralise those who work in the affected area. Failure to take seriously a complaint relating to security could tempt someone to leak information as the only means of getting the matter taken up at higher level.

1815. Where a security problem is dealt with in the early stages it is often possible to resolve the matter without detriment to the individual or the MOD.

Security Education and Training

1816. This should be a continual process. Full guidance on the responsibilities which befall a HOE may be found in JSP 440 Volume 1 Chapter 13. The requirement for annual refresher training being at para 1342. See also para 1824 below.

Aftercare

General

1817. Aftercare is defined at para 11 in the Introduction and in more detail at para 0337. The full background is contained in the MPS Chapter 4.6.

Incident Reporting by Establishments

1818. Should information become available that raises doubts about an individual's suitability for access to protectively marked or sensitive assets, regardless of whether a security clearance is held, the circumstances are to be reported to the relevant vetting unit. In the case of the Armed Forces, both uniformed and civilian staff, the report is to be submitted as an Aftercare Incident Report (AIR). An example is at Annex C.

1819. In considering the need for an AIR, care should be taken about forming judgements on what may appear to be isolated incidents or circumstances that seem to have little relevance to security. Such factors may take on a wholly different perspective when considered together with other information already held by the vetting authorities. In general, matters of fact are always to be reported and suspicions should only be reported when, if they were to be verified, they would cast serious doubt on an individual's security reliability. Annex A provides advice on factors to be considered in relation to an individual's security reliability.

1820. If a character weakness adversely affects an individual's professional performance or conduct, it is essential that the HOE completes an AIR (or its equivalent) in addition to setting in train the necessary administrative or disciplinary action. Vetting actions are never a substitute for, or an alternative to, management action.

Young Personnel

1821. Young personnel who find themselves in a sensitive environment require special supervision. Their lack of experience and maturity may cause vulnerability in a number of areas. The responsibilities of handling highly sensitive information may not always be appreciated at a time when they are still not fully acquainted with their environment and its overall security standards. When DV clearance is granted to a person under the age of 21, special vetting aftercare measures are put into place. These measures will include the nomination by the HOE of a suitable supervisor, to monitor the subject's character and conduct. Instructions for this supervision are set out at Annex B.

Annual Security Appraisals

1822. A Security Appraisal Form (SAF) is to be initiated annually on each person holding a DV clearance. One is also to be initiated on all SC cleared personnel who are STRAP SECRET readers. Further details may be found in JSP 440 Volume 5, Chapter 4. The SAF is to be completed by the subject's first reporting officer under

the umbrella of vetting confidentiality. Responsibility for triggering the SAF process currently varies between Sectors. Following collocation of the DVA and IT recruitment-engineering, it is anticipated that it will be centralised within the DVA. The content of the SAF contributes to a person's vetting record and will be of value at the next review of security clearance. The suggested format for a SAF is at Annex D.

Change of Personal Circumstances

1823. Whenever an individual who holds a security clearance marries, remarries or sets up a stable unmarried relationship, living with someone as a couple, or reports a change of co-residents, the subject's security clearance has to be revalidated. This is done through the medium of security questionnaire MOD Form 1126. The HOEs responsibility towards this aspect of aftercare is given in paras 0335 and 0336.

Conflicts of Interest

1824. On occasions, Service personnel, MOD civil servants, contractors' employees or one of their close relations may come to notice as having been implicated with an organisation or belief which is incompatible with military service or with access to protectively marked assets or to MOD establishments or sensitive sites. This information should be reported, in writing, without delay to the respective Principal Security Adviser. The report should be protectively marked to indicate the content and/or potential sensitivity of the case.

Subversion

1825. Any indication of subversive activity, interest or belief is to be reported, without delay, to the respective Principal Security Adviser in accordance with Service Command/TLB instructions. Should there be an overt, prima facie, case of disciplinary significance, then appropriate investigation will need to be instigated. However, a security vetting interest will remain and the circumstances should be reported as indicated in para 1818 above.

Countries to which Special Security Regulations Apply (CSSRA)

1826. Comprehensive details of the HOEs responsibility in relation to persons travelling to CSSRA and to contacts with CSSRA nationals are set out in Chapters 21 and 22.

Treatment by Psychiatrists and Hypnotherapists

1827. HOEs should be aware that before a person who holds a security clearance seeks treatment from, or a consultation with, a psychiatrist or hypnotherapist, specialist advice is to be taken from the relevant Service or civilian medical authority and from the respective vetting unit.

Hypnotic Entertainment

1828. The employment of hypnotic entertainers in Service establishments is not to be encouraged. This is because individuals under hypnosis are neither in control of their faculties nor able to recall what they may have said or done. Such a situation is deemed to be incompatible with the responsibility associated with the holding of a security clearance. Annual security lectures should bring out the dangers inherent in hypnotic entertainment

Breaches of Security

Physical Security – Losses and Recovery

1829. For details see JSP 440 Volume 1 Chapter 5 para 05939 to 05942.

Documentary Security – Losses and Compromise

1830. For details see JSP 440 Volume 1 Chapter 2 para 0235 – 0249.

ANNEX A

NOTES FOR GUIDANCE WHEN CONSIDERING AN INDIVIDUAL'S SECURITY RELIABILITY

Vulnerability

1. These notes are intended to help identify factors that may render an individual susceptible to pressure or improper influence, or otherwise indicate unreliability. Some of the most obvious of these are:

a. Financial problems, including unexpected wealth.

b. Use of illegal and/or addictive drugs.

c. Alcohol abuse.

d. Sexual offences, eg paedophilia.

e. Suspicion or evidence of sexual behaviour which is in conflict with conditions of service and/or could give rise to pressure from a third party.

f. Illegal or injudicious behaviour, particularly when living or travelling abroad.

g. Compulsive gambling.

h. Any illness or mental condition which may cause significant defects of judgement.

i. Involvement with extreme political groups as described in the Statement of Vetting Policy at Annex 3A.

Warning signs

2. It is not possible to produce a definitive list of the sort of problems to look out for because individuals vary and what might be considered a potential danger signal in one person might be considered relatively normal for another. However, it is very important to be alert for any signs of significant and potentially worrying aspects or changes in a person's behaviour or lifestyle and, if any such changes occur, to report them immediately and not wait for the next periodic formal review of the individual's security reliability. In some cases, slight signs that all is not well, particularly if they become more obvious when a person is under pressure, may indicate the beginnings of a serious security problem.

Possible signs of drug and alcohol abuse

3. Some of the signs and symptoms listed below, when taken in isolation, may be of no significance, or may be symptomatic of illness which has no security significance. However, when several such symptoms manifest themselves together, the commander/line manager will wish to consider whether matters are sufficiently serious as to merit the attention of the Principal Security Adviser. Unless the matter is clear-cut, the commander/line manager should endeavour to have a sympathetic chat with the person concerned with the aim of discovering what lies at the root of the problem, before deciding whether to consult the relevant Principal Security Adviser. Even if the case is not so referred, it may still be appropriate to refer the individual to welfare, medical or counselling services.

Drugs

4. An apparent change in personality or general attitude to, for example, family, colleagues or work.

5. Unexplained inadequate or uneven performance, particularly when indicated by:

a. erratic timekeeping;

b. disregard for discipline.

6. Personality changes such as:

a. furtive behaviour;

b. stealing;

c. frequent attempts to borrow money;

d. obvious familiarity with slang expressions for drugs and the methods of taking them;

e. wearing sunglasses in inappropriate situations (some illegal drugs contract or dilate the pupils of the eye to a marked extent);

f. attempts to keep arms covered even in hot weather (to hide needle marks);

g. frequent visits to the lavatory or some other secluded area on a long-term basis which cannot be attributed to known illness (to provide an opportunity to take drugs);

Alcohol

7. Inadequate or uneven performance at work particularly indicated by:

   a. lack of concentration;

   b. loss of interest;

   c. afternoon lethargy;

   d. unexplained absences during the working day;

   e. unreliability and forgetfulness;

   f. reluctance to accept responsibility;

   g. oversensitivity to criticism;

   h. poor timekeeping.

8. Physical deterioration such as:

   a. bleary eyes;

   b. slurred speech;

   c. flushed face;

   d. unsteadiness;

   e. hand tremors;

   f. smell of alcohol on the breath in the morning;

   g. frequent sick leave, explained as minor illness, especially when it occurs often on Monday mornings.

. Personality changes such as:

   a. moodiness;

   b. anxiety;

   c. depression.

This page intentionally left blank.

ANNEX B

GUIDELINES FOR NAMED SUPERVISORS OF PERSONNEL AGED UNDER 21 OCCUPYING DV POSTS

Introduction

1. The role of the supervisor of personnel working in sensitive areas is a particularly important one and this is especially so where young people are concerned. It is not always possible to avoid employing personnel under 21 years of age in sensitive areas. Where it proves to be unavoidable, special care is needed to ensure the close supervision of such personnel, who are at an impressionable age and whose character, interests and opinions are likely still to be developing.

2. The responsibility for the supervision of under 21s filling DV annotated appointments is placed on named supervisors, who are directly responsible for the close supervision of the staff assigned to their control. The aim of these guidelines is to provide a supervisor with a clear understanding of what the role entails and what needs to be done to carry out the duties effectively.

Close supervision

3. A supervisor will be expected to get to know the individual well and to keep in sufficiently close contact with him to be able to discern any potential problems and any changes in his behaviour or attitudes and to bring them to the attention of his HOE without delay. This process will require supervisors to be sensitive to the personal problems and concerns of young staff, and be prepared to listen sympathetically to them and to encourage them to seek help in resolving any problems they may have which, if unchecked, could lead to difficulties in the future.

What to look for

4. Guidance is given in Annex 18A. The vetting authority will advise on what steps, if any, should be taken to keep a problem under both control and review.

Formal duties and specific controls

5. There are certain formal procedures which a supervisor, must ensure are carried out. These include the following:

a. **Limitations on access to sensitive material.** Apart from the standing need to know principle, the access of young staff to, and

involvement with, protectively marked and sensitive assets must be limited until the supervisor has formed a judgement as to their reliability and discretion. Even then, access to the most sensitive information and material should continue to be limited, as far as is practicable.

b. **Limitations on areas of responsibility.** Personnel under 21 should not be given sole responsibility for putting away papers and securing protectively marked or sensitive assets at the end of the day and for opening secure areas at start work, at least until such time as a judgement can be formed as to their reliability and discretion.

c. **Problems for shift workers.** It is recognized that in a shift-working environment there may be particular difficulties in implementing the measures outlined in these guidelines, not least because changes in shifts could well result in supervisors having little contact with individuals. In such cases, an assistant supervisor must be appointed. However, even when a supervisor's role is shared, the principles governing supervisory responsibilities will remain the same and there will be a need to exercise no less care in carrying out these duties because they are being shared.

d. **Regular reports.** DV clearance for individuals under 21 years of age is subject to annual and other reviews. During such reviews, the supervisor will be required to provide a report on the individual's general reliability and character (a SAF may be used for this purpose). At the final review both the subject and his immediate superior officer will be interviewed.

e. **Detachments.** Should the individual be detached to another establishment, it is vital that the supervisor arranges for the receiving establishment to be notified that the individual holds a higher level security clearance and that, being under 21 years of age, is subject to these special procedures.

f. **Postings and transfers.** Should the supervisor or the individual be posted, the former must notify the local security officer that the individual is subject to these special procedures.

ANNEX C

RESTRICTED - VETTING [1](when completed

From: .....To: DVA

.....

.....

.....Date: .....

AFTERCARE INCIDENT REPORT (AIR)

No: ..... Rank/grade: .....

Name: ..... Initials: .....……

Establishment/Unit:.....Regt/Corps:.....

1. The security clearance of the above named is[2] .....

2. The following incident concerning a person of security interest is reported.

3. Employment and authorised access to protectively marked material[3]:

.....

.....

4. Details of incident and assessment of effect on the subject security reliability[4]:

.....

.....

.....

.....

5. Assessment of the risk to security that may result from the subject's continued access to protectively marked material:

.....

.....

.....

RESTRICTED - VETTING [1](when completed)

6. Details of action already taken to limit the subject's access to protectively marked material, and of any disciplinary or administrative actions taken or being considered:

.....

.....

.....

.....

.....

7. Recommendation of HOE/Commander[5]:

.....

.....

.....

.....

.....

Signature[6]..... Name & Initials: .....

Rank:.....Appointment:.....

Contact Telephone Numbers: (Service).....(Civil) .....

Establishment/Unit/Branch stamp

Copy to:

PsyA who, if there is a need to know, will advise subordinate Security staffs on a "Personal for" basis

RESTRICTED - VETTING [1](when completed)

RESTRICTED - VETTING [1](when completed)

Notes:

1. In addition to the descriptor VETTING, the *minimum* protective marking given to this report is to be RESTRICTED.

2. Insert the current security clearance of the subject ie SC, DV or none.

3. Insert current employment and level of access and, if known, future employment with date and level of access.

4. Full details of the incident are to be included; where appropriate, any supporting documents (eg supervising officers' reports) are to be attached.

5. Include a recommendation by the HOE/Commander as to whether SC or DV should be denied/withdrawn/suspended pending investigation.

6. When the incident gives rise to a recommendation for suspension/withdrawal/denial of a clearance, the HOE/Commander is to sign the report personally. In other cases this task may be delegated.

RESTRICTED - VETTING [1](when completed)

This page left intentionally blank

ANNEX D

RESTRICTED (when completed)

SECURITY APPRAISAL FORM

To: DVA **From:** [Establishment]

Ref: [Establishment Ref] **Date:**

Details of subject

Surname: ..... Forenames: .....

Rank/grade: ..... Service/staff No: .....

Post: ..... Date in post: .....

Security Appraisal

1. How long has the subject served under your control?

   ..... years ..... months

2. Are you satisfied with the subject's attitude toward security? YES/NO

If No, please explain why:

3. As far as you are aware, has he/she been responsible for any breaches of security during the last 12 months? YES/NO

If Yes, please give brief details if they are known

RESTRICTED (when completed)

RESTRICTED (when completed)

4. To the best of your knowledge, has he/she shown any evidence of:

a. Associations or contact with subversive organizations of British or foreign origin? YES/NO

b. Misuse of drugs? YES/NO

c. Misuse of alcohol? YES/NO

d. Unreliability, dishonesty, untrustworthiness or indiscretion? YES/NO

e. Significant financial difficulties? YES/NO

f. Conduct liable to lead to vulnerability to blackmail (e.g. sexual or other)? YES/NO

g. Illness, including mental illness, which might cause defective judgement? YES/NO

5. If you have answered YES to any of the elements of Question 4 above, please give brief details:

6. How well is the subject known to you outside of normal working hours?

WELL
SLIGHTLY
NOT AT ALL

7. Are you aware of any other grounds for doubting the subject's suitability for continued DV clearance? YES/NO

If Yes, please give details:

RESTRICTED (when completed)

8. Please provide a general assessment of the subject's character and reliability:

Signed: ..... Name: .....(Block capitals)

Rank/grade: ..... Post: .....

Tel no and ext: .....

Note: If, by completion of this form, you have highlighted any concerns about the subject's continued suitability for access to highly sensitive material, you should consult the security officer and consider the need for an Aftercare Incident Report to be raised.

RESTRICTED (when completed)

This page intentionally left blank

SECURITY ADVICE ON TRAVEL

This page intentionally left blank.

CHAPTER 19

SECURITY ADVICE ON TRAVEL

Introduction

1901. Overseas travel can present a variety of security risks. This chapter contains general security advice on travel. Where additional regulations apply, this is indicated in the text.

Security Advice

1902. The relevant points of contact for security advice on travel are:

a.	Royal Navy	-	DNSyICP, P1A	27141 PY
b.	Army	-	HQ LAND Phys/Pers Sy (through local Formation HQ G2 staff)	
c.	RAF	-	HQ RAFP&SS, OC FC&T	7035 HEN
d.	Central TLB	-	Hd Pers Sy	Rm 320SY 78568MB 0207 807 8568

In all other cases the TLB PSyA staff should be consulted.

Special Regulations

General

1903. There are special regulations governing travel by Service personnel and MOD Civilians to a number of countries. Advice on where to find further information is given below. In cases of doubt personnel should consult their Establishment Security Officer (ESyO).

Countries to which Special Security Regulations Apply

1904. There are special rules for travel to a small number of countries where the threat from foreign intelligence sevices is particularly high. These are known as Countries to which Special Security Regulations Apply (CSSRA). See Chapter 21 for further information.

Ireland

1905. Guidance on travel to Northern Ireland and the Republic of Ireland is published in Volume 1 Chapter 7 paras 07160 to 07205. This is complemented by single Service travel rules and by special rules for travel to Northern Ireland and the Republic of Ireland for Service personnel.

Overseas Areas of Current Military Operation

1906. The relevant PSyA should be consulted before any travel to overseas areas of current military operation is undertaken.

Foreign Intelligence Services

Threat

1907. Individuals employed by government departments and agencies, the Armed Forces, and List X firms may be of interest to Foreign Intelligence Services (FIS) when travelling overseas. Those engaged in defence, foreign affairs, scientific and technical fields are of special interest even if they are not actually working on protectively marked assets. Attempts may be made to compromise them with the intention of recruiting them or of using them for intelligence purposes.

1908. FIS are most likely to target travellers in the countries on the CSSRA list (see para 1904). But there are other countries of concern, such as some of the states of the former Soviet Union, Bosnia-Herzegovina and South Africa, where travellers are particularly likely to be targeted for intelligence purposes. Western visitors are also likely to attract hostile attention in Iran, Iraq, Libya and North Korea. The threat may be from the local intelligence service, but it is at least as likely to be from that of another country, particularly the Russian Federation Intelligence Services, which may target Western visitors anywhere in the world. A list of countries in which there is a high security threat to MOD visitors from FIS appears at Annex A.

Guidelines

1909. Visitors to the countries listed in Annex A should read Chapter 21 Annex D on methods of intelligence entrapment and comply with its guidance on defensive measures.

Terrorism and Civil Disorder

Threat

1910. Personnel travelling abroad should be aware that in many countries there is a threat from terrorism. This may be directed at British nationals within or visiting a country, the indigenous population, or at other nationals who work in or are visiting the country. In this respect British visitors may become victims of terrorist violence which is not specifically directed at them. In many countries, particularly where there is a sizeable British community or where British military personnel serve, the threat is higher than that in UK and may fluctuate more than UK threat levels.

1911. There is an increasing trend towards terrorism without frontiers. Usama bin Laden, and groups who have allied themselves with him, are the protagonists in this increasingly global threat, posing a threat across most of the developing world, as well as in parts of Western Europe and the US. Irish related terrorism has also been responsible for a number of attacks on British military personnel abroad in the past and this could occur again.

1912. Terrorists may use a number of alternatives to attack a target rather than use direct violence. For example, terrorist groups are becoming increasingly computer literate and are not only using computers for communications, propaganda and the gathering of targeting information, but there is the possibility of them being used to carry out harassment or attacks against the government infrastructure. There is also a steady increase in the number of Westerners who are being kidnapped; however it is difficult to distinguish whether this is for terrorist or criminal motives.

1913. Travellers are most likely to encounter problems of civil disorder in developing countries where civil war and/or insurgency are rife, or where only a fragile system of law enforcement exists.

1914. The threat from terrorism is volatile and it would not be practicable to list here the countries where there is a particular threat since the list would quickly become out of date. Travellers should consult the MOD Monthly Threat Assessment (see para 1917) for the terrorist threat and check FCO Travel Advice about civil disorder and other matters (see para 1918).

Guidelines

1915. General guidelines for security against terrorism when travelling can be found in Volume 1 Chapter 7 Annex O.

Responsibility of Individuals

1916. Service personnel and MOD Civilians must comply with the special regulations for travel to certain countries (see paras 1903-1906). Service personnel must also comply with any single Service instructions on travel. Otherwise there is no requirement for staff to seek security permission to travel to any country, including those at Annex A, and normally no formal briefing or debriefing will be necessary. However, if anything of security concern arises while the traveller is in any foreign country, he must report as soon as possible after returning the full circumstances to his ESyO.

Action before Travelling Overseas

1917. Before travel arrangements are made, advice should be sought about the general threat to safety in the country concerned. Specific advice is available

through ESyOs, who have access to the Monthly Threat Assessment signal issued by the MOD, which is also available on the MODWeb.

1918. The FCO Travel Advice Unit also provides advice to travellers on threats from terrorism and civil disorder, and on health, travel regulations, and other matters. This advice can be obtained from:

a. The appropriate ESyO

b. BBC 2 Ceefax, page 470 onwards

c. The FCO Travel Advice Unit, London

Tel: 0207-238-4503/4

Fax: 0207-238-4545

d. Internet: http://www.fco.gov.uk/travel/default.asp

ANNEX A

COUNTRIES IN WHICH THERE IS A HIGH SECURITY THREAT TO MOD VISITORS FROM FOREIGN INTELLIGENCE SERVICES

1. In addition to the Countries to which Special Security Regulations Apply (CSSRA) (see Chapter 21), there is also a high security threat to MOD visitors in the countries listed below from the local intelligence service or from that of another country, especially the Russian Federation Intelligence Services.

Armenia	Azerbaijan
Bosnia-Herzegovina	Georgia
Iran	Iraq
Kazakhstan	Latvia
Libya	Lithuania
North Korea	Poland
South Africa	Syria

Note. Amendments to this list will be notified periodically by D Def Sy, usually in a DCI(Gen).

This page intentionally left blank.

NOTIFICATION OF SECURITY CLEARANCES FOR TRANSFERS, DETACHED DUTY AND EXCHANGES

CHAPTER 20

NOTIFICATION OF SECURITY CLEARANCES FOR TRANSFERS, DETACHED DUTY AND EXCHANGES

Introduction

2001. This chapter deals with the notification of security clearances for MOD personnel involved in both internal and external transfers. Many of the internal notification procedures are heavily dependent on single-Service administrative methods which are exclusive to each area. The scope of this chapter, therefore, provides only the broad, departmental requirements which will have to be amplified in other orders and instructions. The overall provision, which must apply to this area, is that without the requisite level of assurance of probable reliability (Basic Check) or security clearance no access to sensitive information or assets is to be allowed.

Transfers, Loans or Moves to Another Department, Agency or Company

2002. Anyone with a current security clearance can carry his clearance with him if he moves or is transferred or loaned to another department, agency or company. Responsibility for ensuring that the security clearance meets the appropriate criteria rests with the IMPORTING SECTOR. Thus, the importing sector will ensure that the current clearance is suitable for use in its area of responsibility. If the appropriate level of clearance has not been held, has lapsed or is close to expiry, the exporter is responsible for doing the mandatory investigative work, and the importer will then make the final assessment of the findings to judge suitability for transfer. For the conditions governing the transfer of a security clearance, see para 2018.

2003. In all cases, the receiving organisation has the right to examine the security papers relating to an individual before accepting him on transfer or loan. If the individual requires Developed Vetting (DV) clearance, the relevant papers must be examined before the transfer or loan takes place. If the transferee does not have appropriate clearance, it is the responsibility of the receiving department to ensure that the correct level of clearance is obtained. This should be achieved before the transfer takes place. However, where this is not possible, the subject can be accepted at the discretion of the Head of Establishment.

2004. If a Security Check (SC) or a Counter Terrorist Check (CTC) is required, it is normally sufficient for the receiving department to be given a written assurance that clearance has been granted for the level required and that no information of security vetting significance exists.

2005. If the supplying department has, in its records, information supplied by the Security Service, such information is not to be passed to a receiving department outside the MOD without prior reference to the Security Service.

Employment and Courses with NATO or other International Organisations

2006. Treaties and other international agreements and protocols usually require an agreed level of security vetting assurance before employment or attendance on courses takes place. It is therefore important that the posting authority or civilian personnel management authority (CPMA) consults the PSyA/DVA as appropriate at the earliest stage of the appointment process. Often special vetting requirements may call for some additional form of vetting or, at least, a special international defence organisation (IDO) security clearance certificate. Annex A outlines the format for a NATO security clearance certificate and, unless otherwise required (see para 2008 for WEU requirements), this format may be used suitably amended, without NATO terminology, for other international organisations.

2007. Certificates are to be sent to the single Service element (where one exists) of the formation or unit concerned or to the receiving NATO agency, before the arrival of the subject. NATO security clearances are not required for personnel filling national appointments who have access to NATO SECRET or COSMIC TOP SECRET material, provided that the appropriate national level of security clearance is in issue.

Employment with Western European Union (WEU)

2008. At Annex B is an example of the dedicated security certificate, referenced RS100, which is to be used for those taking up employment under WEU auspices. RS100 is to be completed by the respective vetting authority and sent to the Security Officer, WEU Planning Cell, 4 Rue de la Regence, 1000 Brussels, c/o UKMILREP, BFPO 49. RS100s must reach Brussels before individuals arrive in post.

Postings, Temporary Duty or Detachments to Foreign Countries

2009. Posting authorities, CPMAs or temporary duty sponsors are to ensure that the individual to be moved is in receipt of the appropriate level of security

clearance and that the level is properly notified to the receiving PSyA well before the movement takes place. Certification is to be made as appropriate (see para 2006).

Postings: Potential Conflicts of Interest while on Military Operations outside the UK

2010. The policy to be followed is set out in Annex 20C.

Postings, Temporary Duty or Detachments within the MOD

2011. Notification of levels of security clearance for postings within MOD may normally be made without reference to the security vetting papers. Under such circumstances, a suitable notification of security clearance to the receiving establishment's security officer is sufficient. However, should the receiving area require a more detailed assurance of vetting standard, then that assurance may be validated by the receiving area's vetting authority.

2012. For temporary duty and detachments a simple notification, in signal or certificate format, will be sufficient. For guidance, SC clearance is normally held by:

a. All RN officers and ratings.

b. All RM officers and marines.

c. All Army officers and retired officers (ROs).

d. All RAF officers and airmen.

e. Non-industrial civil servants working in the MOD and for the RN, RM and RAF.

2013. Should there be any aftercare elements associated with the clearance in issue, the parent vetting authority is to consider the need for onward briefing to the receiving area.

Notification of Security Clearance within Parent Organisation

2014. The procedures are set out in paras 0819 and 0917.

Foreign Nationals Serving, Detached or on Temporary Duty with HM Armed Forces

2015. Foreign nationals serving with HM Forces will only do so after suitable international agreement between the countries concerned. Security clearances which equate to our national levels of access will normally be notified by the foreign embassy to D Def Sy InfoSy(IVCO) and thence to the host PSyA. Similarly, security clearances in respect of overseas students will be processed by the Directorate of Foreign and Commonwealth Training (DFCT) and notified to the training establishment(s) and PSyA's concerned.

2016. Security clearances of members of foreign forces on detachments or other forms of temporary duty will usually be notified on a reciprocal basis to that detailed in paras 2006 and 2007.

2017. In the absence of any form of MOD authority, no access to sensitive assets or information is to be given to foreign nationals. Similarly, even if such exchange of information is authorised, it is not to proceed without suitable assurances of security clearance.

Factors Governing the Transfer of a Security Clearance

2018. The following conditions must be applied when transferring a security clearance:

a. Initial and revalidated DV and SC security clearances must not be more than seven or ten years old respectively.

b. There must not have been **more than one year** between leaving one organisation and joining another.

c. The individual must not have resided overseas for more than six months in that year.

To avoid misunderstandings, sector security authorities and civilian management may well need to promulgate these rules down to their appointing/drafting/posting authorities.

ANNEX A

NATO UNCLASSIFIED

Nato Personnel Security Clearance Certificate

To: (Receiving Unit)

_____

Certification is hereby given that:

1. Full name……

D.o.B and Place:…… has been granted a personnel security clearance by the Government of the United Kingdom in accordance with current NATO regulations, including the Security Annex to C-MOD(64)39 in the case of ATOMAL information and is, therefore, declared suitable to be entrusted with information classified up to and including *(Note 1):*

…….

2. The validity of this certificate will expire not later than:……

Signed:…….Rank/Grade:……..

Title:…….Date:……

Official Government Stamp

NATO UNCLASSIFIED

Notes:

1. ***Level of Access:*** *Insert, as appropriate, one or more of the following:*

(a)	*COSMIC TOP SECRET*	*(d)*	*COSMIC TOP SECRET ATOMAL*
(b)	*NATO SECRET*	*(e)*	*SECRET ATOMAL*
(c)	*NATO CONFIDENTIAL*	*(f)*	*NATO CONFIDENTIAL ATOMAL*

(If 'ATOMAL' clearance is shown, the classification is to be qualified by the words 'SUBJECT TO INDOCTRINATION').

2. ***Expiry Date:*** *the date of expiry for this certificate is NOT to be later than 5 years after the date of issue of EITHER the subject's*

a) Last SC security clearance or review, or

b) Last DV security clearance or review as appropriate

3. ***Government Stamp.*** *Insert the relevant official stamp.*

4. ***Despatch of Certificate.*** *Detach this tear-off slip (notes 1 to 4) prior to the despatch of the certificate.*

This page intentionally left blank.

ANNEX B

WEU SECURITY CERTIFICATE (RS100)

This is to certify that:

Surname and
forenames:……

Date and place of
birth:…….

is the holder of a security clearance established by the Government of:

…….

in conformity with current WEU regulations and may receive classified information up to and including:

……

……

The present certificate expires on: ……..

Signed:……

Rank/Grade……

Date:……

Official Government Stamp

This page intentionally left blank.

ANNEX C

POSTINGS: POTENTIAL CONFLICTS OF INTEREST WHILE ON MILITARY OPERATIONS OUTSIDE THE UK

Introduction

1. In any developing crisis involving operations outside the UK, personnel with the ability to speak the local language(s) and provide local knowledge will invariably be at a premium and be required at short notice. Those best able to meet this remit and to fill key operational posts will often be those with parental or other ties in the country(ies) concerned. This may give rise to potential conflicts of interest which cannot be investigated through the normal security vetting process. Frequently, there will be insufficient time to complete the full DV procedure, even where this is justified, before the individual has to deploy. There may be a risk, therefore, that some individuals in key positions with particular attributes may become liable to pressure once deployed.

Aim

2. To ensure that individuals in the categories outlined in above are properly briefed and debriefed when posted to key appointments on overseas operations in a time of crisis.

Executive Action

3. At the outset of certain (eg. peacekeeping) operations outside the UK, all subordinate commanders are requested to ensure that the following actions are carried out:

a. **Pre-Deployment**

(1) The identification of individuals assessed to be particularly at risk.

(2) The briefing of individuals at risk about likely pressures that could be brought to bear.

b. **Post-Deployment**

(1) The debriefing of all those briefed (vide para 2012 a.(2)).

Responsiblities

4. Responsibilities are allocated as follows:

a. **DVA:** Following nomination by posting authorities for Service personnel or by CPMAs for civilian staff, the identification of individuals likely to be subject to pressure.

b. **Intelligence Corps Unit, Local P&SS Unit, D Def Sy, ESyO** as appropriate:

(1) Pre-deployment briefings.

(2) Post-deployment briefings.

(3) Ensuring that copies of the briefing/debriefing reports are passed through the relevant security staff chain to the DVA for enclosure on the individual's security file.

Promulgation

5. These instructions should be brought to the attention of relevant staffs at regular intervals and implemented whenever sensitive operations outside the UK are mounted.

SECURITY DIRECTIONS FOR COUNTRIES TO WHICH SPECIAL SECURITY REGULATIONS APPLY (CSSRA)

This page intentionally left blank.

CHAPTER 21

SECURITY DIRECTIONS FOR COUNTRIES TO WHICH SPECIAL SECURITY REGULATIONS APPLY (CSSRA)

Introduction

2101. In recent years, Arms Control Inspections, the NATO steered Partnership for Peace (PfP), OUTREACH and other confidence building programmes have significantly increased contacts with foreign nationals. Such contacts have the potential for giving rise to serious security concerns and require special security measures and awareness, particularly if the contact involves nationals of a country which has not yet reformed its political system.

The Threat

2102. Service personnel and MOD civilians, regardless of their rank, grade and level of security clearance, are of potential interest to many Foreign Intelligence Services (FISs). Included on the agenda of most FISs is the assimilation of scientific, defence and technological information as well as biographical information on individuals for possible exploitation at a later date. It is naïve to assume that friendly countries would not be interested in such information as there is fierce competition between rival defence contractors because national and financial stakes are so high. FISs may recruit agents who are nationals of a third country or they may deploy their own staff posing as nationals of a third country. Clearly, there is a need to exercise due caution when dealing with any foreign national and for a strict general application of the 'need to know' principle. Annex D lists FIS methods of entrapment etc.

Aim

2103. The aim of this chapter is to provide guidance on the security measures to be taken by all who have contact with nationals of CSSRAs during official or private travel to such countries or when using their airlines, overland transport or shipping companies.

Application and Definitions

2104. These directions apply to all personnel of the RN, Army and RAF, members of the Reserve forces, officers of Military Cadet forces and members of the MOD Civil Service. Where civil servants or Service personnel are employed by a Service other than their own, they are also to follow any local instructions that may be

promulgated by their host Service, which itself has a duty to keep the parent PSyA informed about travel approved for their attached personnel.

2105. These directions do **not** apply to Service personnel taking part in overseas deployments or to organisations managed by a defence contractor. Exceptionally, pre-notification of visits is **not** a requirement for staff involved with Arms Control activities but compliance with all other security rules is mandatory. Security controllers concerned about the special threat posed by foreign countries to the Government assets that they hold should obtain advice from the contracting authority.

CSSRA

2106. In this chapter countries in which foreign intelligence services pose a particular threat to UK interests are termed Countries to which Special Security Regulations Apply (CSSRA). A list of such countries is at Annex A and also appears in Defence Council Instructions (General). This list is updated from time to time. In drawing up this list, no account is taken of the danger posed by local terrorist groups or of the degree of civil unrest which may be encountered in the countries concerned. Threats of this nature can change very quickly and our source of protective security information is the Foreign & Commonwealth Office Foreign Travel Unit in London.

The CSSRA List

2107. No public comment should be offered about the content of the CSSRA list. However, the appropriate PSyA may wish to draw on the following in response to enquiries:

> "It has long been the practice for government departments and agencies to advise employees of the problems that they may encounter when travelling overseas. This is for the protection of both government assets and the employees themselves. Departmental advice is based on central guidelines which are kept under regular review, but it is for each department or agency, having regard to the nature of its work, to decide whether restrictions should be imposed in relation to any particular country or category of employees."

Security Point of Contact

2108. For the purposes of these instructions the relevant points of contact are:

a.	Royal Navy	-	DNSyICP, P1A	(27141 PY)
b.	Army	-	HQ LAND Phys/Pers Sy (through local Formation HQ G2 staff)	(3412 SM)
c.	RAF	-	HQ RAFP&SS, OC CSC	(7035 HEN)

d.	Central TLB -	Hd Pers Sy	Rm 320SY 78568MB (0207 807 8568)
e.	DLO	DLO Sy AI	68418EN

Note: DLO staff in the first instance contact their unit security officer.

f.	DPA	DPA PsyA	30620ABW
g.	PJHQ	SO1 J2	PSyA 46145NW

In all other cases the TLB PSyA staff should be consulted.

Foreign Contacts

Contacts made in the UK

2109. Chapter 22 deals with the security measures that cover personal contacts established during visits, both official and when on leave, by all foreign nationals to the UK and to MOD bases overseas.

Contacts made Overseas

2110. The security measures in this chapter are aimed primarily to cover contacts made in CSSRAs and have been drawn up to protect the individual from action by FISs, extremist groups, investigative journalists and criminals. Some of the circumstances in which contacts could be made by FISs are listed Annex B. Our defensive security measures embrace:

a. Assessment of the risk posed by the contact.

b. Briefing individuals about the threat to their security which may result from a future encounter and an emphasis on the need to safeguard protectively marked information, particularly that of high level.

c. Counter-measures to be employed by the individual.

d. Recording, centrally, that the contact has taken place along with any significant intelligence or security information which becomes apparent.

Reporting Contacts

2111. Any incident or circumstance that gives rise to security suspicion about a foreign contact is to be reported without delay to the ESyO for investigation by the appropriate authority. Such investigation may result from any significant

professional or social contact in the UK or overseas with a national of CSSRA especially if an attempt is made to:

a. Request a significant favour or get one involved in illegal activities.

b. Obtain biographical or employment information about oneself, or any other person.

c. Recruit an individual for any intelligence purpose or engage in any behaviour giving rise to the suspicion that the foreign national concerned is a member of a FIS, security organisation or other group posing a threat to the individual.

Annex E gives sample headings for reporting contacts.

Travel to, or through, CSSRAs

2112. Personnel travelling to, or through, a CSSRA or who travel in transport operated by such a country are vulnerable from a security point of view. Security precautions are, therefore, necessary.

2113. Any significant contact with nationals of a CSSRA, while abroad on a duty or private visit as an individual, or with a group, is to be reported to the nominated SyO of the official group, or to the ESyO of the parent unit on return to UK or base overseas. If the ESyO deems the contact to have been significant or suspicious he is to report the facts to the security point of contact without delay. The security point of contact is to arrange all appropriate follow-up action.

2114. The responsibilities of individuals and sponsors of groups in relation to travel are:

a. **Individual travel.** Whether a member of the Armed Forces or an MOD civil servant, each person is responsible for carrying out the instructions set out in this chapter.

b. **Official group travel.** The sponsor of the journey is to appoint an officer to carry out the instructions in this chapter for the group unless other directions have been issued by sectors, for example, to cover travel by a large group of personnel. When a large group of personnel travel to a CSSRA, it is particularly important that the names of DV cleared staff are notified to the security point of contact beforehand. Each individual is responsible for ensuring that the sponsor is aware of his obligations in relation to the journey, particularly if members of the group are cleared to DV level or are subject to special intelligence induction regulations

c. **Other Government Departments (OGD).** When travelling with personnel employed by an OGD, different arrangements may have to be made to take account of special dispensations granted by that Department to

their staff. In such circumstances, the individual is to consult the appropriate security point of contact.

Action before Travel to CSSRAs

2115. Before travel arrangements are made, advice should be sought about the general threat to one's safety in the country concerned. The source of such information is the FCO Travel Advice Unit and can be obtained from:

a. The appropriate security point of contact (see para 2108 above).

b. BBC 2 Ceefax, page 470 onwards.

c. The FCO Travel Advice Unit, London.

Tel: 0207 238 4503/4

Fax: 0207 238 4545

d. Internet: http://www.fco.gov.uk/travel/default.asp

2116. A check should also be made with the travel agent or with the Embassy of the country concerned about entry visa requirements. Medical and inoculation advice can be obtained from a GP. Before travel arrangements are paid for the permission of the appropriate security point of contact should be sought for the journey to be undertaken, in the light of duties on which the subject is, or has been engaged. See also para 2117, where the sub-paras explain the requirement to inform, or to obtain permission from, the security point of contact before travel arrangements are made. STRAP inducted personnel should also refer to JSP 440 Volume 5 Chapter 4 Annex E paras 26 to 28.

a. **All personnel** due to make an outward visit to any of the CSSRA are to inform their ESyO. This should be done at the earliest opportunity and, normally not later than fourteen working days in advance of the visit. The ESyO will then notify the security point of contact at once and preferably by fax. The proforma at Annex C may be adapted by Sectors to suit their specific needs. The security point of contact will normally respond to such requests by phone or in writing with five working days.

Note: Individuals working in Intelligence compartments are to clear their desire to travel well in advance with their controller who should then advise the appropriate security point of contact whether such travel should be approved. In both cases, such advice should be entered on the proforma at Annex C. The fact that a person is STRAP inducted is protectively marked CONFIDENTIAL and the proforma at Annex C should be upgraded if that is the case.

b. **DV postholders.** Such personnel are deemed to be seeking *permission* to travel. Application should be made a minimum of three weeks before travel arrangements are finalised and paid for. The security point of contact will notify the result of the travel application and outline the defensive briefing and debriefing arrangements required. All DV holders should be aware that by travelling to CSSRAs their future intelligence appointments may be affected.

c. **DV cleared personnel** (other than those covered by sub-para 2116b above) are deemed to be *advising* the security point of contact of their intention to travel. The security point of contact will notify the result of the travel application and outline any briefing and debriefing arrangements required.

Note: There are no restrictions additional to those in para 2116b for SAO, STRAP 1 and STRAP 2 inducted personnel. Other intelligence compartments may have additional travel restrictions; compliance with these is the responsibility of the individual and of the relevant compartment controller.

d. **SC cleared personnel** are to follow the procedure detailed at para 2116c above.

e. **Non List X Contractors' Employees** cleared to SC level or above should inform the relevant security point of contact through their sponsor or project manager of their intention to travel to a CSSRA and thereafter submit a report about any suspected FIS action or topic of security interest.

Duties requiring Regular Travel

2117. Certain personnel, such as those in the Army whose duties require them to travel to CSSRAs regularly may be in frequent contact with citizens of those countries. Such personnel are only required to report their circumstances to their local HQ. Permission is needed from their CO or HOE to have frequent CSSRA contacts, or for related travel, only by those who have received special intelligence briefings. Special arrangements are in force for the Arms Control organisation (JACIG) and members of the RAF air transport force which are administered by HQ RAF P&SS OC CSC.

International Appointments

2118. As well as forwarding full details about their intention to travel to a CSSRA, Service personnel and MOD civil servants serving in international appointments (eg. NATO, UN and European Union etc) are to consult their local UK National Security Authority for advice. They are then to comply with these instructions as modified by any international regulations that may apply.

Debriefing

2119. All personnel who have travelled to any of the CSSRA are to be debriefed by their ESyO or other body nominated by their Command on their return, as follows:

a. **Mandatory** debriefs are required for DV postholders. The resultant reports are to be submitted by the ESyO or other nominated body, by letter or fax (see Note) to the security point of contact.

b. **Optional.** In the case of DV personnel **not** covered above and of SC personnel, a note should be sent by the ESyO to the security point of contact if there is something significant to report for enclosure on the subject's security file. If a more comprehensive report is necessary, a debrief is to be conducted by the ESyO and the resultant report is to be sent by letter or fax (see Note) to the security point of contact outlining the facts.

Note: Faxed reports up to RESTRICTED are acceptable within Great Britain but secure mail must be used for Northern Ireland, British Forces Germany and all other overseas bases.

Travel to the People's Republic of China (PRC) but NOT the Special Administrative Region (SAR) of Hong Kong

2120. In addition to the reporting requirement described at para 2114, clearance for travel to the PRC including Macao but **excluding** the SAR of Hong Kong, is required from MOD Sec(O)2 for:

a. Personnel at unified Grade 7/Captain RN/Colonel/Group Captain and above.

b. Any visit by a significant group (10 or more) of Service personnel irrespective of rank.

2121. Annex F contains advice based on the Security Service pamphlet Security Advice for Visits to China, and Annex G contains advice from the Security Service pamphlet Security Advice for Visits to Russia and the former Soviet Republics.

This page intentionally left blank.

ANNEX A

COUNTRIES TO WHICH SPECIAL SECURITY REGULATIONS APPLY (CSSRA)

Belarus

China – Note 1

Federal Republic of Yugoslavia – Note 2

Russia

Ukraine

Notes:

1. Includes Tibet, Macao and the Special Administrative Region (SAR) of Hong Kong.

2. The Federal Republic of Yugoslavia comprises Serbia and Montenegro.

This page intentionally left blank.

ANNEX B

THE PRINCIPAL CIRCUMSTANCES IN WHICH CONTACTS ARE MADE BY FOREIGN INTELLIGENCE SERVICES FOR INTELLIGENCE PURPOSES

1. The principal circumstances are:

   a. Contacts in the course of duty.

   b. Visits to CSSRA.

   c. Business or commercial activities with a bona fide organization which involve contact with a person who could acquire information about, or provide some hold over the subject as a result of a transaction, for example, insurance, a loan or hire purchase.

   d. Exhibitions, sporting events, scientific conferences, professional and cultural meetings.

   e. Social occasions such as official receptions or private entertainment.

   f. Pen friendships or answering questionnaires or advertisements.

   g. Membership of learned societies.

   h. Amateur radio activities (including the use of Citizen Band radio) or transactions arising from radio broadcasts from these countries.

   i. 'Au pair' or other exchange arrangement or the employment of domestic help from such a country.

   j. Connection to the Internet or comparable networks.

This page intentionally left blank.

ANNEX C

RESTRICTED – STAFF (when completed)

Application for approval/notification of intention to travel to, through or use the travel facilities of Countries to which Special Security Regulations Apply (CSSRA).

Surname:……
Forenames:……
Rank/grade/rating:……
Official/Staff No:……
Date and place of birth:……
Unit/Ship/Establishment:……
Country(ies) to be visited:……
Reason for visit:……
Duration of visit:
From……To……..

a. Are you visiting privately or as a member of an organised group?

b. If latter, which organisation?

c. Names of any travelling companions.

d. How do you intend to travel? Air, sea, road, rail or combination?

e. Do you propose to use travel facilities of a country presenting a special security risk?

f. Have you any relatives resident or employed in the country(ies) you propose to visit? If so, give details:

g. Are you now or have you recently been inducted:

h. In connection with your proposed visit are you aware of any other matters which may present a security concern?

Signature: Date:

RESTRICTED – STAFF (when completed)

RESTRICTED – STAFF (when completed)

ESTABLISHMENT/UNIT SECURITY OFFICER

Signature:……..

Date:……

ESTABLISHMENT/UNIT/SHIP:……..

RESTRICTED – STAFF (when completed)

ANNEX D

METHODS OF INTELLIGENCE ENTRAPMENT AND DEFENSIVE MEASURES

The Targeting of Visitors by Intelligence Services

1. The methods of intelligence entrapment described in the following paragraphs are of particular importance with regard to the CSSRA listed at Annex A.

2. All MOD Service and civilian personnel (regardless of the degree of security clearance which they may hold) should be aware that they may become objects of interest to the intelligence service of any country listed in Annex A from the time that they file their visa application with the consulate of the country concerned.

3. Having identified a person of interest, an intelligence service may seek to gain a hold over that person while they are in the country concerned as described in paragraphs 4 to 11 below.

Surveillance, Eavesdropping and Clandestine Entry

4. MOD Service and civilian personnel (the visitor) should be aware that local people such as guides (particularly if they are English speaking), drivers, hotel staff, touts and loiterers in tourist resorts commonly act as informers or workers for the local intelligence service. A visitor may, therefore, effectively be under surveillance for much of the time. Hotel rooms, or the apartments of acquaintances made locally may be subject to eavesdropping by concealed microphones and/or surveillance by cameras. It may also be assumed that telephones, particularly in hotels, will be subject to bugging. Visitors should give no indication that they are aware of such operations. They must not search for any devices or make any acknowledgement of the fact should a device be found accidentally. Hotel rooms may be clandestinely entered and searched. All papers relating to a visitor's work should be left at a secure location.

Entrapment Ploys

5. Because of the control which the local intelligence service may achieve as a result of the methods described above, visitors must take special care not to break local laws. They must conduct themselves in such a way as not to lay themselves open to blackmail or pressure. Visitors must realise that in these countries the legal authorities work closely with the intelligence service. "Ploys" which may be used to trap the unwary are described below.

Alcohol and Drugs

6. In many countries, drinking alcohol is an accepted form of social behaviour. However, excessive consumption of alcohol can render an individual susceptible to garrulousness, injudicious and anti-social behaviour and possible arrest by police. Personnel must avoid drunkeness. The use of, or association with, illegal drugs or drug pushing in CSSRA can easily lead to far greater complications and is now well known as a form of entrapment.

Sexual Involvement

7. Intelligence services use the threat of exposure, following sexual involvement with a local, in order to blackmail visitors into working for them. The intelligence services may "arrange" the liaison itself, or may exploit a spontaneous liaison. Visitors should be wary of entering into any friendship which might attract the attention of the local intelligence service. Homosexual acts which are legal in the UK may be contrary to local laws.

Currency Transactions

8. It is dangerous for a visitor to get involved in illegal currency deals. Apparently highly advantageous offers to change the local currency for Western currency are probably illegal and may be arranged by the local intelligence service. Intending visitors are advised to obtain the latest information on currency regulations from a reputable travel agent, bank or state tourist office of the country concerned before leaving the UK. These regulations are likely to change and fresh enquiries should be made before each visit.

Blackmarket Goods

9. Local laws may forbid the sale or purchase of certain goods and deals of this kind may be exploited by the local intelligence service. Visitors should not be tempted into deals involving the sale of any consumer goods which they have brought with them. Antiques and religious objects may be subject to stringent local laws on export and visitors must ensure that they have the correct permit before attempting to take these out of the country.

Correspondence and Literature

10. Local laws may prohibit the import or export of certain types of correspondence or literature. Visitors must be careful about the type of literature they bring into the country and be very wary about requests to take out correspondence or other literature with them when they leave. The possession of

these items could lead to prosecution and subsequent pressure to co-operate with the local intelligence service.

Existing Relationships with those of Local Origin

11. Those who are themselves related, or who are related by marriage, to persons who originate in one of the countries listed in Annex B must take particular care

when travelling to the country concerned. The local intelligence service may put pressure on the visitor through their family. Persons in this category will be of special interest to the local intelligence service and, even if the partner of an official has obtained British nationality, he or she must realise that in the country concerned they may no longer be under the protection of the UK as the country may not acknowledge any change of nationality. Holders of dual nationality will be in a similar position.

Photography

12. Unthinking use of a camera can lead to misunderstanding. The taking of photographs and video films should be restricted to places which are normal tourist attractions. Local sensitivities may be offended by taking photographs and films of poor or less developed areas. The taking of such photographs, or of photographs near military installations or prohibited areas could lead to accusations of involvement in espionage and exploitation by the local intelligence service. When in doubt about taking a photograph visitors should ask first.

Defensive Measures

13. Visitors may be exposed to security dangers if they are detained by the local authorities as a result of failing to avoid any of the pitfalls outlined above or as a result of infringing any local law or traffic regulation. A person thus involved may be approached by the local militia or the local intelligence service which might seek to extract a promise of co-operation with the authorities in exchange for an undertaking that no charges will be preferred. Such undertakings should not be given if they can be avoided. Legal documents admitting to wrongdoing or to a misdemeanour should not be signed unless under an intolerable stress or on the advice of an official from a British mission. A visitor must report the situation as fully as possible to the local UK consulate at the earliest possible opportunity. On return to the UK, the visitor must make a full report, in writing, of the incident in question to their security point to contact. A full and honest report, even if to the detriment of the visitor, will neutralise the possibility of blackmail.

14. During travel visitors should:

a. Not divulge information about their employment or place of work.

b. Whenever possible avoid carrying papers relating to their work. Official papers and/or passes are not to be taken on holiday.

c. Whenever possible travel with companions who are well know to them.

d. Avoid areas where there is unrest or civil disturbance.

e. Never enter a prohibited zone.

f. Avoid making controversial statements.

g. Be alert to potentially compromising situations.

h. Be careful not to break local laws.

ANNEX E

FORM OF REPORT FOR SIGNIFICANT CONTACTS MADE WITH NATIONALS OF COUNTRIES TO WHICH SPECIAL SECURITY REGULATIONS APPLY (CSSRA)

1. In drawing up reports of such contacts the following information should be considered and offered in as much detail as is relevant:

a. General information:

(1) Name of host or correspondent,etc.

(2) Whether the contact was by chance or pre-arranged.

(3) Names of other persons to whom introduced.

(4) Whether previously acquainted (if so, give details).

(5) Address or location of contact or meeting place.

(6) General remarks on subject discussed.

(7) Details of any requests for, or discussion about, protectively marked information or material or the nature of your work.

(8) Details of any invitation to continue a social relationship.

(9) Nature of any entertainment undertaken.

b. Information about each person met or corresponded with:

(1) Physical appearance.

(2) Mental attitudes.

(3) Behaviour and demeanour.

(4) Political inclinations.

(5) General interests.

2. Whenever possible, an identifying photograph should accompany the report with the person indicated by a mark on the photograph and sufficient information on the back to identify the person, the environment, the occasion and the date.

ANNEX F

TRAVEL BRIEF FOR VISITORS TO CHINA

Introduction

1. China is now one of the world's fastest growing economies. And, despite the difficulties of working there, many foreign companies are eager to join the increasing number of those who are investing their time, money and effort in establishing links with China.

2. The purpose of this brief is not to discourage the development of trade, nor to warn against the financial and legal pitfalls of working in China which, incidentally, are many! This brief gives advice about Chinese intelligence activity and how you can guard against the risks it might pose to you when visiting China.

Chinese Intelligence Aims

3. Chinese intelligence activity is widespread and has a voracious appetite for all kinds of information; political, military, commercial, scientific and technical. It is on this area that the Chinese place their highest priority and where we assess that the greatest risk lies.

4. The Chinese have realised that it is not productive to simply steal technology and then try to 'reverse engineer it'. Through intelligence activity they now attempt to acquire an in-depth understanding of production techniques and methodologies. There is an obvious economic risk to the UK. Our hard earned processes at very little cost and then reproduce them with cheap labour.

5. It is also, potentially, more serious than the above. In certain key military areas China is at least a generation behind the West. The Chinese may be able to acquire illegally the technology that will enable them to catch up. The real danger is that they will then produce advanced weapons systems which they will sell to unstable regimes. They have a track record of doing so. The consequences for the world's trouble spots and any UK involvement there could be disastrous.

Characteristics of Chinese Intelligence Activity

6. Chinese intelligence activity is very different to the portrayal of 'Moscow Rules' in the novels of John Le Carre. The Chinese make no distinction between 'information' and 'intelligence'. Their appetite for information, particularly in the

scientific and technical field, is vast and indiscriminate. They do not 'run agents' – they 'make friends'. Although there are Chinese 'intelligence officers', both civilian and military, these fade into insignificance behind the mass of ordinary students, businessmen and locally employed staff who are working (at least part-time) on the orders of various parts of the State intelligence gathering apparatus.

Cultivation

7. The process of being cultivated as a 'friend of China' (ie. an 'agent') is subtle and long-term. The Chinese are adept at exploiting a visitor's interest in, and appreciation of, Chinese history and culture. They are expert flatterers and are well aware of the 'softening' effect of food and alcohol. Under cover of consultation or lecturing, a visitor may be given favours, advantageous economic conditions or commercial opportunities. In return they will be expected to give information or access to material. Or, at the very least, to speak out on China's behalf (becoming an 'agent of influence').

Locally Engaged Staff

8. Most companies operating in China are obliged to employ a number of locally engaged staff supplied by organisations such as the 'Provincial Friendship Labour Services Corporation'. It is probable that the Chinese civilian intelligence service will have briefed such staff to copy all papers to which they are able to gain access. Many Chinese students and some businessmen also work to a brief from the Chinese intelligence services.

Technical Attacks

9. The Chinese intelligence services are known to employ telephone and electronic 'bugs' in hotels and restaurants. They have also been known to search hotel rooms and to use surveillance techniques against visitors of particular interest.

Compromise

10. The Chinese intelligence services have been known to use blackmail to persuade visitors to work for them. Sexual involvement should be avoided, as should any activity which can possible be construed as illegal. This would include dealing in blackmarket currency or Chinese antiques and artefacts, straying into 'forbidden' areas or injudicious use of a camera or video recorder.

What you should do

11. This brief has warned you about the aims of Chinese intelligence activity and indicated some of the means they use to obtain intelligence. The steps you take to protect yourself, your department or agency, your company and the UK are up to you.

12. Common sense will tell you to be careful in your dealings so that you do not give away more than you mean to, or find yourself in a position where you will feel obliged to do more for the Chinese than you know you ought. Careful use of the telephone and postal system will prevent you from giving away free information. By avoiding indiscreet and injudicious behaviour you will prevent yourself from being compromised. If the worst case happens, and you are arrested and charged, or if you have been caught in an embarrassing situation you should always insist on being immediately allowed to contact the British Embassy immediately.

This page intentionally left blank.

ANNEX G

TRAVEL BRIEF FOR VISITS TO RUSSIA AND THE FORMER SOVIET REPUBLICS

About this brief

1. The purpose of this brief is to provide security advice for travellers to Russia and the rest of the former Soviet Union (FSU). It describes both the risks involved in travelling to Russia and the other former Soviet Republics, and the action to be taken should trouble arise. The information in the brief is based on the actual experiences of recent travellers to the FSU.

Why should I read this brief?

2. As a visitor to Russia and the FSU you may attract the attention of the local security and intelligence services. Although most travellers experience little or no trouble, it would be unwise for you to assume you are immune to this attention. As you will see from the examples given in this brief, all visitors to Russia and the FSU are potentially of interest to foreign intelligence services, irrespective of the purpose of the visit.

What are the RFIS after?

3. In view of the poor state of the Russian economy, the Russian Federation Intelligence Services (RFIS) place a high priority on information to bolster their economy, scientific and technical information, and on information to help advance their political influence. This extends to the theft of patents and to seeking detailed information on Western scientific developments. They also have an interest in political reporting, alongside their more traditional targets such as Western Defence and Security, eg NATO. The SVR (foreign intelligence service) and the GRU (military intelligence) try to recruit British subjects to work for them in the United Kingdom and elsewhere, often initially in minor support roles. They are always on the watch for any British subject who may be induced, either wittingly or unwittingly, to cooperate. They do not necessarily concentrate on those who already have access to information of value to them.

The approach to Overseas Visitors

4. From the moment a visitor enters the country, he or she may be reported on by a wide variety of people, including officials, business contacts, tourist guides, hotel employees and apparent casual contacts. People who speak the visitor's own language may be introduced in such a way as to make him think that it was the visitor who took the initiative, or that their meeting was entirely fortuitous. We know it sounds like a spy movie, but as well as having wide networks of agents and informers, the FSB (Russian security service) makes extensive use of sophisticated technical devices. In the main hotels all telephones can be tapped and in some rooms visual or photographic surveillance can be carried out, if necessary using infrared cameras to take photographs in the dark. If is perfectly possible for the FSB to ensure that the visitor is placed in such a room. There is also a wide range of technical devices, which can be used outside and even in places such as restaurants and cars. These technical devices pick up indiscreet talk which could be of use to the FSB.

Methods of Compromise

5. Careful behaviour should be sufficient to avoid difficulties with the FSB, but visitors should bear in mind that they can get into trouble in many ways. Unofficial financial transactions, such as obtaining local currency at favourable rates or selling personal possessions to acquaintances, are all in contravention of local laws. A Russian friend or acquaintance may ask a visitor to deliver a letter or a present to some relative living in the West, but this is again in breach of local regulations. Taking works of art out of Russia is a serious offence, while drink-driving regulations are rigorous. There are strict rules about taking photographs in Russia and it is advisable to find out in advance where cameras may be used.

6. Irregularity in personal behaviour may also lead to trouble. The FSB may attempt to capitalise on sexual liaisons between visitors and local nationals. In addition, the FSB may attempt to compromise and subsequently blackmail through knowledge of marital infidelity or sexual activity the target may wish to hide.

Risk of Arrest

7. A visitor who commits any offence against local laws runs the risk of being arrested and threatened with the withdrawal of business facilities, imprisonment or exposure unless he or she agrees to work for the FSB. Attempts may be made to induce the victim to sign a confession or to agree to cooperate. Alternatively, the evidence may be stored away for use at a later date, perhaps when their circumstances have changed (for example, after the visitor has married, or entered a different field of employment).

8. Visitors may face any of these hazards whenever they visit Russia but the FSB is especially active during Trade Fairs. At these times particular care should be taken.

SVR and GRU Approaches Worldwide

9. As a general point, it should be borne in mind that both the SVR and GRU are known to have approached British nationals, in particular businessmen, in many parts of the world. The threat is especially high in some Third World countries where the RFIS believe they have little to fear from the local security services. People who have been regular visitors to Russia are more likely to come to notice since the FSB will hold some record of their personal details, which can be passed onto the SVR and the GRU. An indiscretion or irregularity committed in Russia, even if apparently unnoticed at the time, may be exploited by RFIS officers elsewhere. In addition, RFIS officers may make approaches using the cover of another nationality, for example Eastern European or Scandinavian, to disguise their true allegiance.

Advice about visits to Other Former Soviet Republics

10. Visitors to the other former Soviet Republics should heed the advice given to visitors to Russia. Although these republics now have their own independent security services, many of them continue to cooperate closely with the RFIS. The RFIS are so comfortable operating in some former Soviet Republics that they regard them as virtually home territory. The advice about compromising offences and risk of arrest also applies. It should be noted that many of these republics are not used to Western visitors and may pay particular attention to them.

Final Point

11. Visitors to any foreign country should remember that it is in their own interests to tell the British authorities abroad (the Embassy, High Commission or Consulate) or the Police at home if they have been in trouble, or if they suspect that a foreign intelligence service is interested in them. Anything they say will be treated as strictly confidential and advice on how to avoid any further difficulties will be offered.

General Security Advice

12. Knowledge of the risks can do much to help the visitor to Russia avoid difficulties. Every visitor should:

a. Remember that occupation and background afford no immunity from the attentions of the FSB;

b. Be careful about personal behaviour. Visitors travelling alone are at considerably greater risk of an approach than those travelling groups who then stay together;

c. Practice sensible security procedures. Guard sensitive documents and be careful when, where and with whom you discuss sensitive topics;

d Be alert to compromising situations. Any visitor who is charged with infringing local regulations or caught in a personally embarrassing situation should insist on being allowed to contact the British Embassy immediately.

SECURITY DIRECTIONS FOR INCOMING VISITS BY ALL FOREIGN NATIONALS

This page intentionally left blank.

CHAPTER 22

SECURITY DIRECTIONS FOR INCOMING VISITS BY ALL FOREIGN NATIONALS

Introduction

2201. In recent years Arms Controls Inspections, the NATO steered Partnership for Peace (PfP), the UK initiative on OUTREACH and other confidence building programmes have significantly increased contacts with foreign nationals. Such contacts have given rise to serious concerns about security and have stimulated the measures outlined in this chapter to safeguard our protectively marked information and the security integrity of the individual.

2202. Many foreign intelligence services (FISs) are interested in UK service personnel and MOD civilians, regardless of their rank, grade or level of security clearance. They are primarily concerned with accumulating scientific, defence and technical information as well as biographical information about individuals, for possible exploitation at a later date. Intelligence organisations of friendly countries are also interested in such information because the financial and sometimes national stakes involved are so high. An intelligence organisation may recruit agents who are nationals of a third or may deploy their own staff posing as nationals of a third country. Caution is needed when dealing with any foreign national and the 'need to know' principle must be closely observed.

Aim

2203. The aim of these directions is to outline the security procedures covering incoming visits by all foreign nationals (including those from CSSRAs).

Application and Definitions

2204. These instructions apply to all personnel of the Royal Navy, Army, Royal Air Force, members of the Reserve forces, officers of Cadet forces and MOD civil servants. They also apply to MOD List X contractors and their employees. Where civil servants or service personnel are employed by a Service other than their own they are to follow any local instructions that may be promulgated by their host Service.

2205. Spare.

2206. The term 'visitor' in these instructions means any person who is **not** a British national and is **not** a person described in para 2207.

2207. These directions are **not** applicable to the following foreign nationals:

a. All exchange officers or overseas liaison officers who work in the Armed Services, MOD HQ buildings, at the Defence Evaluation and Research Agency (DERA) sites or with List X defence contractors.

b. Certain civilians for whom other arrangements, particularly in respect of vetting, apply:

(1) British contractors' employees working in MOD/Service establishments;

(2) Personnel employed or sponsored by other UK government departments;

c. Service and civilian personnel in NATO posts, visiting NATO authorities on NATO business for whom arrangements are provided in the NATO publication, "Security within the North Atlantic Treaty Organisation".

d. Private guests attending social functions.

Sponsor

2208. This term 'sponsor' is used to describe the MOD or other Service authority which endorses the requirement for each visit by a foreign national.

Security Point of Contact

2209. For the purposes of these instructions the relevant points of contact (POC) are:

a.	Central TLB	- D Def Sy Info Sy(IVCO)	80130 MB
b.	Royal Navy	- DNSyICP,SOICP	27145 PY
c.	Army	- HQ LAND Phys/Pers Sy	3412 SM
d.	RAF	- HQ RAF P&SS, OC CSC	5709 RM

In all other cases the TLB PSyA staff should be consulted.

OUTREACH and Partnership for Peace

2210. The security measures to be followed for all OUTREACH and Partnership for Peace (PfP) visits are outlined at Annex A. Appendix 1 list OUTREACH countries (which include some CSSRAs), and areas of UK activity, while Appendix 2 forms the basis of a security brief for HQ/Unit personnel taking part in the project.

Incoming Visits – Sponsoring

2211. No commitment to sponsor an incoming visit should be entered into unless it is likely that approval for the visit will be forthcoming. As well as endorsing the visit, the sponsor is to establish the degree of access to, and release of, protectively marked information within the bounds of the "need to know" principle.

2212. The sponsor is to provide the relevant security point of contact with the names of the prospective visitors, dates of birth, current employment, place to be visited, the date and purpose of the visit. This information is to be supplied as soon as it becomes available. The security point of contact will then arrange for checks to be carried out with the aim of establishing if there is any evidence to suggest that there is any FIS involvement in the visit. Following authorization for the visit to take place, the sponsor is to arrange for the respective security staff to draw up a relevant security plan. It should cover:

a. The briefing and de-briefing of personnel hosting the visit.

b. Access control, the avoidance of sensitive areas, prevention of over-hearing, document protection arrangements and the shrouding of sensitive equipment.

c. The need for a Limited Technical Inspection if necessary.

d. Arrangements for photography and publicity.

e. Organising visitors' passes and protecting the integrity of the host's passes.

f. Warning personnel about the level of information which can be released and reinforcement of the "need to know" principle.

g. Safeguarding personal information about hosts and their personal possessions.

Press and Media

2213. Staff are not to accept visits by members of the press or media unless such a visit has been cleared with the appropriate public relations and security staff. All telephone enquiries by journalists are to be referred to an appointed public relations officer.

Visits by Foreign Nationals to MOD Establishments in UK or MOD Bases Overseas

2214. Spare.

2215. In particular, nationals of CSSRAs are not permitted to visit MOD establishments in the UK or bases overseas including training areas without official sponsorship from MOD, Command or other subordinate HQ as appropriate.

2216. Applications for visits by foreign nationals not on accreditation lists are covered at para 2219. Exceptions are detailed at paras 2223 and 2229 and are only permitted where separate security arrangements apply to the visit.

Sponsor Authorities for Foreign Nationals

2217. Sponsor authorities for foreign nationals may include:

a. Command HQ or, when necessary, a subordinate unit.

b. MOD – Directorate for Central and Eastern Europe (DCEE).

c. MOD – Procurement Executive (PE).

d. MOD – Sec(NS), Sec(HSF) or Sec(AS).

e. MOD – Director of Foreign & Commonwealth Training (DFCT).

f. MOD – Defence Export Service Organisation (DESO).

g. MOD – Directorate North Atlantic and Western Europe (DNAWE).

Accredited Officials

2218. Certain officials of the London based Defence staffs of Australia, Canada, New Zealand and the United States of America are designated "accredited officials". This means that they are included on an accreditation list authorising their entry to specified MOD establishments. Details are held by D Def Sy, the International Visit Control Office (IVCO) and Lead Commands.

Applications for Inward Visits to MOD HQ Establishments by Nationals from Countries listed at Annex B and from NATO Countries listed at Annex C.

2219. Embassies and High Commissions in London have been instructed to submit official applications on standard forms which provide the details required at para 2211. This should be done at least 21 days in advance to IVCO for security clearance of visits to MOD HQ establishments and to all List X defence contractors. Procedures differ for visits to Service sites (see paras 2220 and 2223). When granted, the level of access that may be made available to overseas nationals will be as follows:

a. **Nationals of countries listed at Annex B** will require clearance for access to any protectively marked information

b. **Nationals of NATO countries** will require clearance for access to protectively marked information at CONFIDENTIAL or above. It follows

that official requests for visits where access to sites or to material is only required at RESTRICTED level or below are **not required**. In such circumstances compliance with local security regulations, such as the need to provide escorts, must not be neglected.

2220. For visits to Service sites, the sponsor of the foreign visitors should apply directly to the respective PSyA. The criteria governing access to such site is as stated in para 2219. See also para 2223.

Applications for Inward Visits to MOD HQ Establishments by Foreign Nationals not from Countries listed at Annex B.

2221. IVCO should be notified by host departments/contractors of any planned visits by nationals of any country **not** listed. The full details of the visitors, para 2222 refers, must also include passport numbers, names of employers and a planned itinerary including full details of information to be released, equipment to be displayed etc). These details must be forwarded at least 21 days before the intended date of the visit so that the necessary approval can be sought. Approval to release protectively marked information to the visitors will only be granted by the relevant TLB in accordance with **Table X**, column (c).

Visits to MOD HQ Offices

2222. For visits to MOD HQ offices by foreign nationals who are not designated in paras 2224 to 2230, IVCO will contact the host branch to confirm the identity and credentials of the visitor following receipt of the appropriate application or notification. IVCO is to be informed about the level of releasable information applicable to the country concerned as given in **Table X**. Should the subjects discussed involve material under the control of other departments, IVCO is to be notified. IVCO will consult the other departments concerned if necessary. If information needs to be released at a higher level than that given in **Table X**, the host department must notify IVCO who will then take action and refer the matter to the Release of Military Information Policy Committee (RMIPC) if necessary. If a proposal for a visit is received by a MOD establishment directly from overseas or by a List X defence contractor, details should be passed to IVCO. They will ask the relevant Embassy or High Commission for the countries listed at Annex B to submit a formal application for security clearance for the visit. Separate action will be taken in the case of other countries (see para 2220).

Visits to Service Establishments

2223. When foreign nationals who are not designated in paras 2224 to 2230 wish to undertake such visits, Command or subordinate unit staff will contact the host branch and confirm details of the visitor following receipt of the visit application. The host branch will also be advised by the Sector PSyA of the releasable level of information for the country concerned as given in **Table X**. If information needs to be released at a higher level, the Command/Lead Command security staff must refer the matter to the RMIPC. If a proposal for a visit is received directly from overseas by a

Command, details should be passed to Command HQ who will ask the relevant Embassy or High Commission (countries list at Annex B) to submit a formal application for security clearance of the visit. Separate action will be taken in the case of other countries (see para 2220).

Overseas Officers Working at Service Establishments

2224. This includes Exchange Officers, integrated and non-integrated officers and liaison officers. Security clearance certificates for the individuals concerned should be forwarded to the appropriate security point of contact if they are working at Service/MOD establishments or with List X defence contractors. It is important that establishments adhere to the regulations governing access to, and release of, protectively marked information.

Requests for Visits to Service Establishments by Foreign Attaches

2225. Separate arrangements exist for the security clearance of visits and attachments to Service establishments which are not the responsibility of IVCO. Guidance to Foreign Attaches on how to request visits to units or arrange training courses are detailed in the MOD 'White Book', issued by the Head of Foreign Liaison Section (FLS) (WH03, 8371 MB) to London based Embassies and High Commissions. This requires the Attaches/Advisors to channel their requests as follows:

a. For visits to MOD HQ units, MOD establishments and the defence industry requests to IVCO with a copy to the relevant FLS section.

b. For all visits to UK Royal Navy, Army or RAF establishments requests go to FLS(Nationality), FLS(A) or FLS(Air) as appropriate.

Attaches who make direct approaches for visits or courses should be referred to the White Book.

Foreign and Commonwealth Students

2226. Attendance of such personnel on UK military courses or those arranged by List X firms is normally arranged through the Directorate of Foreign and Commonwealth Training (DFCT) who will ensure that students hold the requisite security clearance for their course as required by JSP 440, Volume 1, Chapter 11. Separate single Service security instructions may also be applicable. If the protective marking of a course is higher than that set for the release of information to the student's nation by **Table X**, column (c), approval must be obtained via the appropriate PSyA. DFCT will notify both the ESyO at the training facility and the appropriate Command of the security clearance level of the student and send a full copy of his security clearance with an easily recognisable photograph. Where overseas students are attached to MOD establishments, including DERA sites or to contractors' premises whilst attending MOD, single Service or List X company organised training courses, the course Directors must ensure appropriate Command HQ/IVCO is given details of the planned visits or attachments and of the level of

security access allowed. This is to be done in sufficient time for the necessary consultation to take place with all interested parties prior to visit approval being given.

Strategic Defence Initiative (SDI) Programme

2227. Visits to the UK by overseas nationals in connection with the SDI programme are co-ordinated by the SDI Participation Office.

Visits to Nuclear Facilities

2228. Separate arrangements exist for international visits relating to nuclear cooperation agreements. ACSA (Nationality) Sec should be consulted for advice. JSP 440 Volume 4 Chapter 1 contains further information about VIP or media representatives' visits to nuclear facilities.

VIP and Unsolicited VIP Visits to MOD Establishments

2229. Visits which involve overseas Ministers, Chiefs of Staff etc are arranged by the Protocol Office or Defence Export Services (MDS 3d).

2230. For the Central TLB, IVCO will not always receive security details of VIP visitors. It is the responsibility of the host to escort all such visitors at all times and to inform the site PSyA of full names and details of visitors together with the intended date of their proposed visit.

2231. Unsolicited foreign visitors will also not have submitted security clearance details through the visits procedure. This being so, the host will be responsible for informing the site PSyA of the visit at the earliest opportunity and for escorting them at all times.

Arms Control Inspections

2232. Separate arrangements exist for foreign inspection personnel involved in arms control inspection work. Command HQ should be consulted for advice in such cases.

Employment of Au-pairs

2233. Service and MOD employed civilian staff are to request approval, for reasons of security, before employing CSSRA nationals as au-pairs. All such applications are to be submitted to the ESyO for onward transmission to the appropriate PSyA. A completed security questionnaire (MOD Form 1109) should, ideally, accompany each application. Applications covering foreign nationals from CSSRAs (listed in Chapter 21, Annex A) may not be approved.

Enquiries to Obtain Information from Foreign Sources

2234. MOD and agency personnel having a need to obtain written information regarding weapons systems originating in foreign countries should, in the first

instance, contact D Def Sy(S&T). Direct approaches should not be made to foreign arms manufacturers and dealers without the permission of the relevant PSyA.

ANNEX A

SECURITY INSTRUCTIONS FOR OUTREACH AND PARTNERSHIP FOR PEACE

Introduction

1. It is essential that all units take proper security action when engaged in the above activities. OUTREACH is HMG's **bilateral** assistance programme to nearly all countries in central and eastern Europe and a number of Former Soviet Union (FSU) countries. PfP is an assistance programme led and coordinated by NATO. A list of countries covered by OUTREACH is at Appendix 1. The directorate for Central and Eastern Europe (DCEE) and the Directorate of North Atlantic & Western Europe (DNAWE) are responsible respectively for OUTREACH and PfP. Both have agreed that these instructions should be used as a security guide by all Service units or individuals who become involved in such activities, visits or exercises whether required to act as hosts or visitors.

2. All visit sponsors have an obligation to consult the relevant security point of contact about pending visits into the latter's area of concern. The obligation for reporting travel or contact is on individuals except where an official group is concerned in which case a nominated person of the unit or HQ branch involved should act on behalf of individuals in making and keeping contact with his local security section. Overall, the aim is to achieve security but minimise red tape while keeping a record of contacts, names and unusual occurrences.

Security Concerns

3. The principal concern is to protect individuals from the continuing hostile intelligence and long term recruiting activities by Russia and agents in other CEE/FSU countries still linked to GRU, the Russian military intelligence service or SVR, the State intelligence service previously known as the KGB. A further concern is the protection of information particularly that relating to scientific or technical matters and equipment. There is also a need to record centrally, for counter intelligence purposes, contacts made and information obtained.

Action to be taken by Individuals or Unit/HQ Security Sponsors

4. See Appendix 1 for visits to OUTREACH countries, visits by their nationals to the UK or to MOD bases overseas and for any contact anywhere:

a. **Pre-visit lists of Russian names.** It is important that, as soon as they are known, the list of Russian visitors (those of other FSU visitors are not

required) is passed to Command/MOD HQ (site security branch) and to D Def Sy Info Sy(IVCO). It should also be copied to the chain of command. This will enable the Security Service to examine them.

b. **Notifications to local security sections.** When notified about a pending inward or outward visit, all units are to report details to local security staff of sections as soon as possible.

c. **Personal security.** It is essential that all personnel involved in the visit are made aware of the threat as they could become a long term recruitment target. Appendix 2, suitably adapted by sectors, is to be used to brief them.

d. **Information release level authority.** Unless the visit is UNCLASSIFIED authority for the release of RESTRICTED material is to be obtained direct from the respective Service Command/TLB PSyA.

e. **Debriefing.** This is to be undertaken by the ESyO under the guidance of the local security section. If there is any doubt as to how this should be done, the local security section should lead.

APPENDIX 1 TO ANNEX A

OUTREACH COUNTRIES AND ASSOCIATED AREAS OF UK ACTIVITY

OUTREACH Countries

Albania	Latvia
Armenia	Lithuania
Azerbaijan	Moldova
Belarus	Romania
Bosnia-Herzegovina	Russian Federation
Bulgaria	Slovakia
Croatia	Slovenia
Estonia	Tajikistan
FYR of Macedonia	Turkmenistan
Georgia	Ukraine
Kazakhstan	Uzbekistan
Kyrgyzstan	Federal Republic of Yugoslavia

Areas of UK Activity

Defence management reform

Defence staff talks

English language training

High level visits

In-country advisers

Joint military cooperation

Russian resettlement

Seminars, courses and expert visits

Training the Baltic Peacekeeping Battalion

UK training opportunities

APPENDIX 2 TO ANNEX A

SECURITY BRIEF FOR UNIT PERSONNEL INVOLVED IN OUTREACH VISITS OR PFP TRAINING

(The following details may be adapted by Commands to suit their particular purpose)

Introduction

1. This brief is necessary due to your pending visit to, from or contact with, Russians, nationals of the FSU or former Eastern Bloc countries. You need to be aware of the potential dangers that may result from your exposure to the attentions of their intelligence agencies. This brief outlines what is required of you with regard to your personal security and conduct.

2. The conduct of individuals is to be beyond reproach. Behaviour which may cause embarrassment or harm to either the UK, the Service or your guests/hosts (ie. sexual liaisons or excessive drinking) are to be avoided.

Counter Intelligence and Personal Security Considerations

3. **Security of information.** While there are not objections to friendly discussions with your hosts, you must be aware of the danger of passing information to them which might be harmful to British interests. As far as possible, the subjects discussed should be those that are in the public domain. You must take great care when talking to guests from the FSU not to provide them gratuitously with protectively marked and/or sensitive information. Your contacts may include GRU Intelligence Officers who may follow up and exploit any information or opportunity that you give them, possibly many years hence. It is especially important that you do not disclose any information about your war role, future plans, capabilities, intelligence and security or equipment under development.

4. Personal security and conduct. The following rules, properly heeded, will help to protect you and your colleagues from any potentially embarrassing and/or compromising situations that may arise:

a. **Personal details and unsolicited information.** Try to keep details of yourself and your family to a minimum. Report any unsolicited correspondence received to your ESyO/USO. Do not become involved in any unofficial social event or over-indulge in alcohol. You should be aware that various forms of sexual blackmail continue to be among the favoured

methods of entrapment. Apparent chance encounters may not be what they seem to be!

b. **Exchange of gifts.** Do not give or accept any gift unless it forms part of an official arrangement or is of a trivial nature.

c. **Reporting of incidents.** Any incident which involves an attempt at subversion, bribery, blackmail, sexual involvement or a request for personal favours should be reported at the earliest opportunity to your ESyO/USO.

5. **Security briefing.** Personnel will be routinely debriefed under local Command arrangements. However, if you see the need, you may request an interview with your ESyO/USO or local security section. At all times, the "need to know" principles of vetting confidentiality and source protection are strictly observed and any information disclosed will not be communicated outside the offices directly concerned.

ANNEX B

APPLICATIONS FOR INWARD VISITS BY OVERSEAS NATIONALS

Algeria	Israel	Saudi Arabia
Australia	Jamaica	Senegal
Austria	Japan	Singapore*
Bangladesh	Jordan	Somalia
Barbados	Kenya	South Korea
Brazil	Kuwait	Sudan
Brunei, Darussalam	Malaysia	Switzerland
Burma	Mexico	Tanzania
Cameroon	Morocco	Thailand
Chile	Nepal	Tunisia
Ecuador	New Zealand	United Arab Emirates
Egypt	Nigeria	Uruguay
Finland	Oman	Venezuela
Ghana	Pakistan	Zaire
India	Peru	Zimbabwe
Indonesia	Philippines	

* Special arrangements exist for visit requests from Singapore to be passed via the British High Commission.

Note: Connect this annex with para 2219.

This page intentionally left blank.

ANNEX C

LIST OF NATO COUNTRIES

Belgium

Canada

Czech Republic

Denmark

France

Germany

Greece

Hungary

Iceland

Italy

Luxembourg

Netherlands

Norway

Poland

Portugal

Spain

Turkey

United States of America

Note: There is a strong likelihood that a dispensation will be granted to other friendly countries enabling them to undertake visits without making a formal application vide para 2219 b. Such countries may include Australia, New Zealand and Sweden.

This page intentionally left blank.

SECURITY DIRECTIONS FOR VISITS ABROAD ON DUTY OR OFFICIAL BUSINESS

This page intentionally left blank

CHAPTER 23

SECURITY DIRECTIONS FOR VISITS ABROAD ON DUTY OR OFFICIAL BUSINESS

Introduction

2301. Though not directly related to personnel security, it is administratively convenient to cover this subject adjacent to the other chapters on travel.

Aim

2302. The aim of these directions is to outline the security procedures covering visits by UK staff abroad on duty or official business. Chapter 19 contains general security advice on travel abroad.

Application and Definitions

2303. These instructions apply to all personnel of the Royal Navy, Army and RAF, members of the Reserve forces, officers of military Cadet Forces and members of the MOD Civil Service.

Security Point of Contact

2304. For the purposes of these instructions the relevant points of contact are:

a.	Royal Navy	-	DNSyICP, P1A	(27141 PY)
b.	Army	-	HQ LAND Phys/Pers Sy (through local Formation HQ G2 staff)	(3412 SM)
c.	RAF	-	HQ RAFP&SS, OC CSC	(7035 HEN)
d.	Central TLB	-	Hd Pers Sy	78568MB

In all other cases the TLB PSyA staff should be consulted.

Outward Visits by UK Based Personnel

General

2305. The consequences of a breach of security overseas can be more serious and immediate than may be the case in the UK. In unfamiliar surroundings, it is particularly important to ensure that the rules designed to safeguard protectively marked or sensitive material are rigidly observed. Staff must be conscious of their

behaviour, not draw undue attention to themselves and be on their guard to ensure that protectively marked information does not fall into the wrong hands. Before leaving the UK, staff must make themselves fully conversant with the security regulations pertaining to their visit. The following rules, which also apply to sponsored consultants and firms' representatives, cover the protective security of personnel travelling abroad on duty or business.

Requirements of Foreign Governments

2306. Foreign governments insist that visits to their countries which involve the disclosure of protectively marked information are sponsored by Her Majesty's Government. In this way, Her Majesty's Government supports the underlying purpose of the visit and accepts responsibility for any protectively marked non UK information acquired during the visit. Before travel arrangements are made for an overseas visit by an MOD official or by a consultant or firm's representative acting on the MOD's behalf, to discuss protectively marked matters with foreign firms or government establishments, the approval of the foreign government concerned is to be obtained. Even when a visit will not involve the disclosure of protectively marked information, some countries, notably the USA and France, require their prior approval to be obtained if the visit is likely to entail entry to a government department or to the premises of a firm engaged on classified work.

Visits to the USA – ATOMIC Information

2307. Visits to the USA to discuss ATOMIC information are subject to strict procedures. The Atomic Control Officer is to be consulted at least seven weeks beforehand. He must, similarly, be consulted before arrangements are made for visits to commonwealth or foreign countries other than to the USA where these will involve discussion of ATOMIC information.

Security Clearance Applications for Visits to NATO Establishments

2308. When a visit to a NATO establishment in an NATO country is proposed, during which NATO classified information is likely to be discussed, the visit is to be supported by a NATO Personnel Security Clearance Certificate, see Chapter 20, Annex A. Applications for these certificates should be made as follows:

a. **Service personnel.** The ESyO should signal the NATO establishment requesting the certificates and provide security clearances of the personnel involved in the visit.

b. **Service, civilian staff, consultants employed in MOD HQ/DPA and contractors' staff travelling as part of an official MOD party.** Except for visits to NATO HQ Brussels when arrangements in para 2309 apply, applications forwarded to the IVCO should be submitted on MOD Form 800. They should be validated and signed by the ESyO. On receipt of MOD Form 800, the IVCO will process the application and forward a NATO security

clearance certificate to the respective PSyA at the NATO establishment to be visited.

c. **Contractors' employees and other non government personnel not travelling as part of an official MOD party.** Visit requests should be submitted by the company or individual concerned to the IVCO using standard IVCO proforma which are available on request. If discussions, involving MOD protectively marked material, are to take place, the appropriate MOD project authority must give prior authorisation.

NATO HQ Brussels

2309. When visiting NATO HQ Brussels, the following information should be submitted to the appropriate single Service security staff, or to the IVCO for MOD civilians:

Full name

Rank/Grade

Date and duration of visit

Reason for visit (to include NATO committee member or title, eg. UK Del, AC/102)

2310. Sector security authorities are responsible for sponsoring visits to NATO HQs and sites by Australian and New Zealand integrated staff and may also be required to issue NATO clearance certificates for other integrated personnel.

NATO HQ Passes

2311. Passes will normally be available for collection by the visitor at the Main Gate to the HQ NATO compound on production of appropriate identification, eg. passport or ID card. The issue of an annual pass can be arranged by the appropriate PSyA staff on written request for those intending to visit frequently, eg 12 times a year. A passport photograph must accompany the application. It is stressed that if an application for an annual or temporary pass which is to state the official's security clearance has not been processed by the UK Delegation to NATO, the visitor will not be permitted to enter the NATO HQ. The individual's security clearance must be verified before entry. Contractors' employees and other non government personnel not travelling as part of an official MOD party are required to submit visit requests to the IVCO using standard IVCO proforma issued for that purpose. The issue of annual passes can be arranged by the IVCO for such personnel, subject to the provisions described above.

Minimum Notice Periods for Overseas Visits

2312. The minimum notice which must be given to visit the countries shown below excludes the time required for processing and forwarding the application by

authorities in the UK. Delay in notifying the appropriate PSyA will cause difficulties to all concerned, including the possible refusal of the visit by the host nation.

USA	-	8 weeks
Canada-		6 weeks
Germany	-	7 weeks
Spain	-	6 weeks
France	-	5 weeks
Italy	-	4 weeks
Norway	-	6 weeks
Netherlands	-	4 weeks
Other countries	-	4 weeks
NATO HQ	-	2 weeks

Other Regulations

Countries to which Special Security Regulations Apply

2313. There are special rules for travel to a small number of countries where the threat from foreign intelligence sevices is particularly high. These are known as Countries to which Special Security Regulations Apply (CSSRA). See Chapter 21 for further information.

Ireland

2314. Guidance on travel to Northern Ireland and the Republic of Ireland is published in Volume 1 Chapter 7 paras 07160 to 07205. This is complemented by single Service travel rules and by special rules for travel to Northern Ireland and the Republic of Ireland for Service personnel.

Overseas Areas of Current Military Operation

2315. The relevant PSyA should be consulted before any travel to overseas areas of current military operation is undertaken.

Personal Security Considerations

2316. Before travelling to any overseas country, advice should be sought about the general threat to personal safety from, for example, terrorism. This information is published and regularly updated by the FCO Travel Advice Unit. Full details on how such information may be obtained is shown in para 1915. Defence Attaches in British Embassies and Defence Advisers in British High Commissions abroad who

will often require notification of pending visits to their country of accreditation are able to provide detailed up to date advice. In cases of duty travel to high risk areas, Security Authorities hold the MOD Overseas Terrorist Threat Assessment List (OTTAL) and are able to arrange an intelligence briefing.

This page intentionally left blank.

INDEX

VOLUME 3
Issue 2

COMMUNICATIONS AND INFORMATION SYSTEMS SECURITY

MINISTRY OF DEFENCE
October 2001

This page intentionally left blank.

VOLUME 3 – CIS SECURITY

CONTENTS

Chapter

Part 2 - Communications And Electromagnetic Security

Part 3 - Acoustic Security

AN INTRODUCTION TO CIS SECURITY

CHAPTER 1

AN INTRODUCTION TO THE SECURITY OF COMMUNICATIONS AND INFORMATION SYSTEMS

Introduction

01001. This Chapter gives guidance on the security of Communications and Information Systems (CIS) in use within Defence and lays down security standards.

01002. CIS Security seeks to protect the data held on CIS by addressing the following:

a. **Confidentiality**. The restriction of information to those authorized to see it;

b. **Integrity**. The preservation of information in its original form unless correctly amended or deleted by authorized people;

c. **Availability**. Having access to the information handled by CIS as and when required.

01003. CIS Security measures within the MOD are designed to address both malicious attack and non-malicious failures and accidents as sources of compromise of Confidentiality, Integrity, and Availability.

01004. Accountability for all aspects of security within MOD, including CIS, rests formally with the Permanent Under Secretary of State (PUS), who has general responsibility for assuring compliance with HMG security policies either directly, or through the Departmental Security Officer (DSO), the Director General Security and Safety (DGS&S).

Applicability

01005. The regulations laid down within this manual represent the MOD minimum ("Baseline") requirements for security of CIS. 'Baseline' in this context means that it is expected that the document will be applied in all cases, unless there are strong, documented, reasons for not doing so. These have mainly been derived from National policy, interpreted to make them more applicable to MOD's various operating environments.

01006. Where certain classes of information are to be stored, processed, or forwarded, the MOD is bound to comply with additional regulations governing their protection,

either in the terms of a bilateral / multilateral agreement (typically for material governed by International Document Organisations (IDO) such as NATO), or as a condition of release (for externally owned or internally compartmented material such as STRAP, as detailed at Volume 5).

01007. If any other cases are identified where an apparent mismatch between the MOD and National policy is identified, it should be assumed that the more stringent requirement should be followed, but clarification should be sought from DDefSy.

Infosec Minimum Standards

01008. Minimum information security standards for HMG are issued under the auspices of the Cabinet Office, either within the Manual of Protective Security (MPS) or as HMG Infosec Standards. These standards are under constant review, and are made available to MOD at TLB level.

01009. Within MOD, these standards are interpreted for the specific Defence environment by this Manual, and may therefore attract a higher requirement than the HMG baseline. Consequently the generic HMG documents should not normally be required as reference documents, although some of the supporting guidance documents, such as CESG Infosec Memoranda, may be directly used by MOD and are therefore directly referenced within this manual.

01010. Should a specific requirement exist which is covered by the generic HMG standards but not by this Manual, DDefSy must be consulted before proceeding.

01011. MOD is committed to implementing information security in a realistic and cost-effective manner, and DDefSy therefore welcomes comments relating to the regulations laid down in this volume, and will take any reasonable issues so identified into consideration when Policy is being reviewed.

Scope and Limitations

01012. This document is primarily intended to address the risk of compromise to official CIS carrying protectively marked data. While it recognises that compromise may arise from accidental as well as malicious causes, it does not cover safety-critical requirements. Such requirements are addressed by appropriate industry standards and regulatory authorities. For the purposes of this document software should be considered safety-critical if its failure would result directly in a hazardous situation. If, however, software failure or compromise would open up a way for a Potential Attacker to create a hazardous situation then it may be considered as security related as well as safety-critical, and this document can apply.

01013. These regulations apply to all CIS owned and managed by MOD, to CIS owned and managed under contract to, or on behalf of, MOD, and to privately owned and contractor owned CIS when carried on MOD or service property, or being used for

Official purposes. This manual applies to all elements of the MOD and Defence Agencies.

Exceptions

01014. This manual does not cover the standards for protection of the financial integrity of data concerned with public and service funds and accounts, which is the responsibility of other authorities and advice should be sought on such matters from the appropriate finance branch.

01015. This chapter does not give guidance on the security requirement imposed by the Data Protection Act. This is laid down in Joint Service Publication (JSP) 406 - Guidance and Instructions Relating to the Data Protection Act 1984 and amended by the Data Protection Act 1988. Guidance on all aspects of the Act can be obtained from the Ministry of Defence Data Protection Office (MOD DPO) based at Minerva House. All systems covered by the Act are to be registered with the MOD DPO together with any claims for exemptions under the Act.

Principles

01016. A CIS is defined as an assembly of electronic communications and/or computer hardware and software configured for the purpose of processing, storing or forwarding information and whose security is the responsibility of a single management.

01017. All CIS that are to be used to process, store or forward Official Information are to be approved by the DSO, through the appropriate security chain of command, to confirm that their use does not present either an unacceptable risk to national security or the operation of the Defence business.

01018. All security depends on a balance of measures to reduce the risk of compromise to an acceptable level. These measures are a number of "facets of security", which are :

- Organisation & Management
- Physical
- Personnel
- Media
- Procedural
- Infosec (Technical **Info**rmation **Sec**urity)
- Compusec (**Comp**uter **Sec**urity)

- ComSec (**Com**munication **Sec**urity)

- RadSec (Electromagnetic **Rad**iation **Sec**urity)

01019. Technical measures can be very complex, particularly for CIS with many users or connected over a wide area. Such systems require careful analysis and the development of individual System Policy Documentation (SPD).

01020. Complexity is very much less for CIS with no external connections, and these, generally referred to as Information Technology (IT) systems form the largest group of systems within Defence.

01021. The early Chapters of this Manual constitute the Baseline needs of such stand alone systems and single personal computers (PCs) with devices for exchanging data on a batch basis and is for the guidance of personnel responsible for their security. The term stand-alone encompasses desktop PCs and portable IT systems, with small numbers of users.

01022. The physical, procedural and personnel measures set out here will apply, as appropriate, to all CIS. More detailed guidance on complex and interconnected CIS is to be found later in this manual.

01023. **Risk Management** The principle of Risk Management is used to adjudge the Countermeasures required to counter the Threats and Vulnerabilities to a CIS, weighted against an Asset Valuation:

a. For Confidentiality, the Asset Valuation is based upon the Protective Marking(s) of the information protected, and security measures relating are a reflection of National Minimum Standards;

b. For Availability and Integrity, the Asset Valuation is based upon the importance of the CIS to both the unit/establishment mission, and for Defence as a whole. This requires the assignment of the Criticality Level (CL) to the system or service, as detailed at **Annex A**.

01024. When performing an asset valuation, it will be necessary to carry out a review of the potential affects of data aggregation on the overall highest the Protective Marking, and similarly of system interconnection on the overall CL of the system-of-systems. Such aggregation should be used within to drive the Risk Assessments carried out, such as those laid down in **Chapter 6** and **Chapter 14**.

01025. Additionally, it is necessary to ascertain whether or not any of the data on the systems is of a purely ephemeral nature, as this may give the Accreditors discretion to reduce the security requirements below that which would normally be required for long term data at the same protective marking level.

01026. In an MOD context, ephemeral data can be considered to be Operational data

with a lifetime of less than 24 hours, or administrative information with a lifetime of less than 1 week.

01027. An issued that can lead to a perceived Aggregation effect is the incorrect application of protective markings to data items. Users are encouraged to review the label, where applied, of any information at the time of its creation, to ensure that this is indeed correct. This is especially important in cases, such as documents with default protective markings embedded in headers and footers, where experience has shown that for many System High systems the default High Water Mark (HWM) is seemingly applied with little apparent regard to the information contain, resulting in either under, or more frequently over, marking. This should be reflected in SyOPs where applicable.

01028. In addressing these requirements it is necessary to have confidence that the security measures implemented will meet these requirements and that there is a degree of trust in these countermeasures.

Release of Information

01029. It is a fundamental tenet of Operations Security (OpSec), that nothing should be revealed to unauthorised persons that could either be of interest to any enemy, or of advantage to an attacker.

01030. As a general principle, therefore, the Techniques, Technologies and Procedures used to secure MOD CIS assets should only be discussed with persons having a direct Need-To-Know (NTK) requirement for this information, in line with the philosophy laid down at Defence Advisory (DA) Notice No. 4, reproduced at Annex B. A technique know as "social engineering" is widely used by "hackers" to obtain the background information they need to attack CIS.

01031. No approach which could lead to the disclosure of information protectively marked CONFIDENTIAL or above to anyone outside the government service is to be made without prior reference to TLB Principal Security Adviser (PSyA) Security Staff.

01032. The use of all Departmental CIS facilities is, and will continue to be, subject to security monitoring. All material held on MOD CIS equipment is deemed to be the property of the Department itself, and staff are reminded that, as a consequence, so-called "private" information held on any Departmental CIS facility will not be afforded any special protection and will be accessible to line management and investigating staff without prior recourse.

Basic Requirements

01033. The protection of information is covered in some detail in other volumes of the Defence Manual of Security. Annex C considers some of the implications, particularly when information is held on IT systems. There are a number of requirements that must

be met before any CIS is allowed to handle official information. The main topics highlighted below give a brief introduction to CIS security.

01034. **Accreditation (Chapter 2)**. Before any CIS is allowed to store, process or forward official information, it must be given security approval, known as Accreditation, which is granted by the Defence Security Standards Organisation (DSSO), PSyA Security Staffs or competent authority. Failure to obtain Accreditation can result in confiscation of the affected CIS.

01035. For systems processing highly Protectively Marked material, or whose operation is Critical to Defence interests, approval may include detailed examination of system specific security requirements agreed between the System Operating Authorities (SOA) and Security staff. Specific rules apply to categories of sensitive material or externally sourced material, generically referred to as Compartmented Information, but often referred to as Codeword material. **In addition to** the requirements for system and site Accreditation from the designated Accreditor(s), approval is also required from the Control or Release Authority before the material may be passed to or stored on the system(s). These rules are covered in detail in **Annex D**.

01036. **Security Policy Documentation (Chapter 3)**. Before accreditation can be granted Security Policy Documentation (SPD) must be produced. The nature of the Security Policy Documentation that is required will be agreed with the accreditor.

01037. Registration (Chapter 3). All CIS, including those handling non-protectively marked data, are to be registered. The registration form will give details of the system, and for stand alone desktop PCs and laptop systems the registration document together with the Security Operating Procedures (SyOPs) fulfils the role of the required SPD set.

01038. **IT Document Security (Chapter 4)**. Protectively marked information held on IT documents; discs, tapes, CDs, microform, printed output etc., must be given a level of protection and control equivalent to protectively marked documents in paper form. Additionally all magnetic media protectively marked SECRET or above must be recorded in a Protectively Marked Document Register (PDR MOD Form 102).

01039. **Disposal of CIS Equipment (Chapter 5)**. When CIS equipment and media becomes surplus to requirement, all protectively marked material that has been processed or stored on these items must not be expose to an unacceptable risk of compromise during disposal.

01040. Illegal Software (Chapter 6). MOD cannot condone the illegal copying of software for use on a MOD system. All civilian and military personnel making, acquiring or using unauthorized copies of software expose themselves to internal disciplinary action and possible criminal prosecution.

01041. **Malicious Software (Chapter 7)**. All CIS must include in their SyOPs specific instructions to counter the threat from computer viruses and other forms of malicious software.

01042. Use of Portable Systems (Chapter 8). Personnel, who use portable systems, including laptops, should be aware that additional security measures are required. These cover the use, interconnection, transport and protection of the portable system.

01043. Deployable Systems (Chapter 9). CIS security on exercises and operations must be appropriate for a range of threats and changes of physical environments. The enforcement of CIS security countermeasures on exercises and operations requires personnel with the appropriate engineering skills, authority, responsibility and training

01044. **Connections to the "Internet" (Chapter 10)**. Before any IT system is connected to the Internet, or similar public data network, permission must be obtained from the DSSO or appropriate PSyA Security Staffs.

01045. Incident Reporting (Chapter 11). All security incidents must be reported, either up the security chain of command, or, for certain types of incident requiring urgent action to nominated specialist reporting points.

01046. Compliance Checking (Chapter 12). In order to ensure that the security measures agreed as part of the Accreditation are maintained, periodic Compliance Checking is carried on behalf of the DSSO, PSyA Security Staffs or competent authority issuing the Accreditation.

01047. Installation Control (Chapter 21). Installation Design Authorities (IDA) are responsible for ensuring that systems are installed in such a manner to not compromise either their own electromagnetic security or that of other systems in their vicinity.

01048. Counter Eavesdropping (Chapter 26). It should always be remembered that any threat related to protectively marked levels of speech, can include audio output from a computer; passwords or personal identification numbers (PIN) called out to other users; and keyboard and printer 'chatter'.

01049. Additionally, there are a number of requirements relating to specific types of equipments that are widely used across Defence.

01050. Telephone Security (Chapter 18). It must be noted that specific rules exist for the use of (speech) Telephony within MOD, and in particular that there are significant controls over the use of both Cordless and Portable (Mobile) telephones.

01051. Facsimile Security (Chapter 19). It must be noted that specific rules exist for the use of both Image and Data Facsimile within MOD.

The Threat

01052. The origins and nature of the threats to official information processed electronically are similar, but not identical, to those to protectively marked information stored and handled in other forms.

01053. An Annual Threat Assessment (ATA) is issued to all Government Departments giving generic statements as to the main sources of Threat. This will include personnel who may be from or influenced by Foreign Intelligence Services (FIS), authorized users who, for whatever motive, may seek to gain access to official information they have no 'need to know', subversive or terrorist organizations, and investigative journalists.

01054. This ATA however is predicated upon a non-military and UK mainland view of the Threat, and consequently does not take into account the varying environments in which the MOD has to operate. MOD's Joint Security Coordination Centre (JSyCC) therefore issues a regular series of bulletins giving a greater degree of granularity, entitled "Information Security Threat Summaries" (ISTS) to Security Staffs, and those seeking detailed information should consult the security chain of command

01055. Additionally, a system of Information Warfare (IW) Indicators Alert and Warning (A&W) levels, analogous to the Bikini/Tahiti/Tesseral alert states for Counter Terrorist and Counter Extremist activity has been defined. JSyCC is responsible for promulgating this information across Defence using a system of Threat Change Notices (TCN). System Operating Authority's responsibilities for acting upon this information are given at **Chapter 2**.

Vulnerabilities of CIS

01056. A CIS is especially vulnerable to attack, because:

a. CIS are designed to be deliberately accessible.

b. CIS are able to store protectively marked data in a concentrated and compact form, where it can be copied, corrupted or damaged quickly and surreptitiously.

c. The aggregation of data may require a higher level of protection than individual items.

d. The supervision and monitoring of activity and personnel on a CIS is more difficult than in an equivalent manual system.

e. Information on CIS can be intercepted where they produce either compromising emanations or they have unprotected communication links.

f. CIS equipment has an intrinsic value and is thus liable to theft in its own right.

01057. The vulnerability of a system can be greatly reduced by good initial planning (which will include the production of SPD), and by the vigorous enforcement of sound SyOPs, reinforced by compliancy reviews, security surveys and inspections, and unit reviews and checks.

01058. Due to the evolution of CIS technologies, and their inherent susceptibility to "bugs" and "design features", new generic technical vulnerabilities are being discovered virtually on a daily basis. Additionally, differing types of CIS platforms will have their own specific vulnerabilities identified. Furthermore, Malicious Software is deliberately designed and promulgated to exploit vulnerabilities, as detailed in **Chapter 7**.

01059. It is therefore necessary for JSyCC to issue warnings about Vulnerabilities (including Malicious Software) to obviate their exploitation by any potential attacker. System Operating Authority's (SOA) responsibilities for acting upon this information are given at **Chapter 2**.

Risk Assessment

01060. MOD policy is that an accreditor, prior to use, must independently assess the security of all information systems. An accreditor requires evidence in order to confirm that the intended use of a system to process, store or forward information does not present an unacceptable risk to National Security.

01061. The effective conduct of MOD operations requires that the security (which includes confidentiality, integrity and availability concerns) of information and services are not subjected to unacceptable risk of compromise.

01062. Formal Risk Analysis and Management methods are now necessary to cope with the complex security problems presented by information systems and networks

01063. It should be recognised that the variety of possible implementations of Physical, Personnel and Procedural measures may require more or less stringent complementary implementation of electronic security measures.

01064. The risk assessment must be agreed by the Accreditor, normally through one of the system / project security management fora. The results should form the basis of all security work in support of the system. Risk Assessment and Risk Management are covered in greater detail in **Chapter 14**.

01065. For systems processing STRAP material, **JSP 440 Volume 5** represents a minimum standard, to be read over and above the requirements laid down in **Chapter 14**.

Registration

01066. With the increasing proliferation of CIS hardware and software assets within MOD it is imperative that details of all such assets are formally recorded. This will assist the DSO and systems/installation managers in accounting for and assisting in the auditing of all devices and software. Furthermore, recording details will aid any investigation should hardware devices be stolen or moved from their approved location.

01067. The format for Registration of systems are given at **Chapter 3**, with a short form being applicable to small systems, and a formalised Project Registration Form (PRF) for larger enterprises.

Security Policy Documentation

01068. Chapter 3 gives guidance on the production of Security Policy Documentation for CIS. This has been subdivided into 2 major elements:

a. SPD for small systems, which is based upon a philosophy of simple Registration provided that the generic documentation provided in Annexes to this Chapter can be complied with;

b. SPD for large and distributed systems, which will have to be specifically written for each CIS in question.

Accreditation

01069. Accreditation can fall into 4 basic categories:

a. **Full Accreditation**. The target for all permanently installed IT systems;

b. **Interim Accreditation.** A constrained authorisation, of limited duration and scope, which has been planned;

c. **Conditional Accreditation**. A constrained authorisation, of limited duration and scope, which has not been planned;

d. **Legacy Approval.** Legacy systems are retained systems. If they are non-compliant with current accreditation practices or security standards, their continued operation has to be accepted on a case by case basis. It is a Government wide requirement that all systems in service on 31 December 2000 are accredited, and hence any systems approved on a legacy basis must be brought up to a standard where at least a conditional accreditation can be issued before that time.

01070. More detailed information on the categories of accreditation are contained in **Chapter 2**.

01071. Complex systems may require the use of formal Evaluation and Certification, as detailed at **Chapter 6,** and this is largely dependant which of one of four distinct modes of operation, known as the Mode of Secure Operation, that the CIS can be categorised as operating within :

a. **Dedicated Security Mode**. A mode of operation in which all the users of a system are cleared for, need-to-know about and have access to all the data handled by it. No Evaluation and Certification will normally be required for such systems ;

b. **System High Security Mode**. A mode of operation in which the users of a system are all cleared for, and have formal access approval for, all the information handled by it, but not all of whom actually need-to-know about all of the data ;

c. **Compartmented Security Mode**. A mode of operation in which the users are all cleared for, but do not have formal access approval for, all the data handled by the system ;

d. **Multi-level Secure (MLS) Mode**. A mode of operation in which a computer system (or network of computer systems) handles data at various protective markings etc, but for which there are users not cleared for all that data and whose access is restricted appropriately.

01072. A special case of Dedicated Mode is Session Processing Mode, which permits the use of a dedicated machine at different protective marking levels of data by using separate media sets. If this method is to be used, the additional paragraphs in **Chapter 3 Annex S** will require to be added to system security instructions.

Integrity and Availability

01073. This policy recognises that for official Information Systems, the protection of integrity and availability merits equal consideration with the protection of confidentiality. It introduces the following new definitions of the two terms -

Integrity: the assurance that information has been created, amended or deleted only by the proper actions of authorised users.

Availability: timely access to assets by authorised users.

01074. The purpose of integrity protection is to give adequate and appropriate assurance against the risk of IT assets being created, amended or deleted other than by appropriately authorised users.

01075. The purpose of availability protection is to give adequate and appropriate assurance against the risk of loss of timely access to IT assets by authorised users.

01076. This policy further recognises that integrity and availability are primarily system or service properties. Integrity and availability protection requirements will normally be assessed at the system level, though specific countermeasures may be applied at lower levels.

01077. **In assessing the protective requirements for official information systems the security objectives of integrity and availability shall be considered alongside that of confidentiality**. The different natures of the three security objectives are recognised but it is acknowledged that failure to safeguard any one of them can result in the compromise of information or other assets.

01078. Integrity and availability protection requirements shall be established for all systems and networks storing, processing or transmitting official information.

01079. The requirements for protection of integrity and availability shall be determined through a risk assessment process, involving IT project staffs and security accreditation authorities as appropriate.

01080. For each of integrity and availability, the risk assessment process shall assign systems to one of two protection requirement ranges, standard or enhanced, and shall consider which supporting security services are relevant. See **Chapter 6 Annex B**.

01081. Countermeasures can be drawn from several different security fields often operating in combination; the two protective ranges are each associated with levels and types of countermeasures that are therefore indicative only (see countermeasures below): protection shall respond primarily to any specific risks highlighted by the risk assessment.

01082. It is recognised that, in the case of certain applications (e.g. in nuclear or air safety contexts), the possible consequences of a loss or compromise of integrity or availability may be so catastrophic that enhanced measures, special to these fields, will always be required even if the threat is assessed as only slight.

Business Continuity

01083. Disruption can arise due to the failure of system components, denial of access or corruption of stored information. Unless planned for, retrieval of data after a disruption is often difficult, time-consuming and sometimes impossible.

01084. Business Continuity addresses what needs to be done to ensure that key activities can survive disruptive events. It involves the identification of priorities and the application of risk management to what has traditionally been termed disaster

recovery. Business Continuity embraces more than just IT: it includes people and processes, accommodation, paper and electronic records.

01085. The major components of Business Continuity are:

a. A Business Impact Analysis to identify the critical areas of work and the activities that support them; to assess the impact of not being able to undertake those activities for given periods of time; and to define what would be needed in order to restore the business to at least its minimum acceptable level.

b. A Risk Assessment to identify vulnerabilities and especially single points of failure. Where appropriate, the risk assessment should identify possible countermeasures.

c. A Business Continuity Strategy drawn from an examination of the options for risk reduction and, should the worst still occur, the options for the recovery of critical business and support.

d. The Implementation of the risk reduction measures and standby arrangements identified in the strategy may be a necessary prerequisite to translating the strategy into a viable set of plans.

e. Preparation of Plans detailing what needs to be done, in the event of a serious disruption, to restore at least the critical functions and processes. There will usually be a set, produced at four levels: a master plan; plans for centrally coordinated activities; service providers' plans; and, locally held, plans for business units.

f. Exercising and maintaining the plans to ensure they are up to date and effective.

01086. Top level Budget Holders are required to ensure that adequate Business Continuity arrangements are in place in their areas. ICS(Pol)BCT under the joint sponsorship of CM(IS) and DGS&S published the Guide to Business Continuity in Defence.

Homeworking

01087. Homeworking is defined as the use of a persons home as their normal place of work using officially supplied equipment. It is often described as working **from** home. It should not be confused with working **at** home which is the term used to describe someone working at home on a strictly temporary basis e.g. during transport disruptions. Staff who regularly work at home for any other reason; eg regular working in the evenings or to collect e-mail, are subject to the homeworking rules.

01088. The specific security rules, which refer to homeworking, are shown at Annex E. The rules for working at home are covered by paragraphs 01089 to 01091 if a privately owned system is to be used; otherwise the rules for the use of a portable IT system as laid down at **Chapter 8** are to be followed.

The Use of Private Computers for Official Purposes

01089. Privately owned systems may be used to process Official information provided that they meet the security requirements applicable to a similar Defence system e.g. they must have an SSP and SyOPs, they must be accredited and have IDA clearance etc.

01090. Security Measures. The rules for IT security stated in this chapter apply, and additionally the following rule also applies. Official information must not be stored on the same physical media as private information or programs. All data used for any purpose on a home computer must be checked for viruses before being introduced to any Defence system by any means.

01091. If any privately owned machine is connected to a communications system, all MOD information must be adequately protected before linking to the system. Furthermore prior approval must be obtained.

Legal Aspects

01092. At present there is no legislation aimed specifically at the security of computers in the government, public, corporate or private sectors. However, there are a number of UK statutory provisions that can be applied to computers, their security and the protection of the data stored on them.

01093. **Official Secrets Act.** This act lays down requirements for the proper control of government information.

01094. Computer Misuse Act. This deals with the rights of computer owners against the unauthorized use of a computer by any party, making offences of attempted or actual penetration or subversion of computer systems. Under the terms of Section 3 of the Computer Misuse Act it is a criminal offence to introduce unauthorized software into a computer system. For the purposes of this instruction unauthorized software is defined as software not obtained via authorized channels. ITSOs are to ensure that only authorized software is loaded and used on systems under their control. This is to be reflected in SyOPs. Additionally, where appropriate and feasible, screen warnings against unauthorised access should be displayed at the system log-on prompt.

01095. Data Protection Act 1984 and Data Protection Act 1998. These are the statutory means of ensuring that adequate security is employed when maintaining records containing personal data. These have been updated as a result of the **European Data Protection Directive**.

01096. Computer Software Copyright. Infringement and copying of Computer Software is governed by the Copyright/Computer Software Amendment Act 1988 and Copyright Designs and Patents Act 1988. Individuals and users should be aware that copyright infringements are not exclusively a matter of civil actions for damages by a copyright owner. The criminal penalties for infringing computer software copyright may include heavy fines, imprisonment (for up to 2 years) and the forfeiture of infringing copies and articles for making them. The Head of Establishment/CO may also be subject to prosecution for permitting illegal software to be used for the processing of official information within the area of their responsibility.

01097. Proprietary software products are usually supplied under a licence agreement that restricts the use of products to specified systems and may limit copying to the creation of back-up copies only. Users and individuals will be acting unlawfully if they use, make, transfer, distribute, translate or adopt any copies of computer software without a licence or the written authorization of the copyright owner.

01098. MOD cannot condone the illegal copying of software, the storage of that illegally copied software in a computer, which would include copying the software into a computer and/or the loading of such software into memory. All civilian and military personnel making, acquiring or using unauthorized copies of software expose themselves to internal disciplinary action and possible criminal prosecution. The use of illegally acquired software in Defence computer and electronic office systems is strictly forbidden. The Head of Establishment/CO is to ensure by regular and recorded checks that IT systems under their control do not contain or use illegally copied software. This should be reflected in SyOPs.

01099. Civil Evidence Act 1968 and the Police and Criminal Evidence Act. These acts define conditions under which computer based evidence may be obtained and used.

01100. Wireless Telegraphy Act 1949. This prohibits the unauthorized use of wireless telegraphy apparatus for the transmission or reception and subsequent disclosure of communications.

01101. Telecommunications Act 1984. This creates an offence of dishonestly obtaining a service provided by means of a telecommunications system, with the intention of avoiding payment.

01102. **Interception of Communication Act 1985.** This prohibits unauthorized interception of communications, with case and time limited exemptions being grantable subject to a warrant.

01103. Public Records Act 1967. This is the statutory provision for the proper care and preservation of documentary records of government activity, ensuring that Departments transfer to the Public Record Office (PRO) sufficient records that describe how they have carried out their functions and duties.

01104. **Human Rights Acts.** This is the statutory provision enshrining the **European Convention on Human Rights**.

Commercial Aspects

01105. As the MOD is the country's largest user of Information Security related products, Users, CIS, and Security staffs can expect to be approached by product vendors wishing to market their product. It is recommend that all such marketing approaches for Information Security related products, other than those already listed in the MOD ICS Catalogue, UK ITSEC approved product list, or similar, be referred to the Defence Infosec Product Coordination Group (DIPCOG) who are charged jointly by DDefSy and CM(IS) with reviewing such products suitability for defence. DIPCOG can be contacted through Hd DefSy(Tech), SY340, 85854MB.

Misuse of Communications and Information Systems

01106. The improper use of MOD CIS will have both a direct and indirect detrimental impact on the MOD's ability to conduct its business effectively and efficiently. The MOD must also meet its legal obligations for ensuring that its employees do not misuse its CIS facilities.

01107. The improper use of MOD CIS has potentially wide ranging ramifications for the Department, its staff, its customers, and others. Even where activities are unauthorised, there may be severe legal and/or financial consequences for the Department. Some of the most serious potential effects are listed below:

a. breaches of national security;

b. breaches of confidentiality (including infringement of personal privacy and breach of commercial confidentiality);

c. disruption to Departmental business activities;

d. damage to Departmental IT facilities;

e. legal cases (libel, harassment etc) brought against the Department;

f. Departmental or personal embarrassment;

g. compromised personal security;

h. infringement of intellectual property rights;

i. use of unauthorised software;

j. harassment of any nature;

k. negligent misstatement.

01108. All staff should be aware that the MOD does not condone, and will not tolerate, the unauthorised use of its CIS. It is committed to preventing instances of improper use from occurring. Where criminal activity is suspected the Department will not hesitate to refer the matter to the Ministry of Defence Police for investigation.

Disciplinary action may be taken against any member of staff who misuses MOD's CIS.

Incident Reporting

01109. Any hardware or software security weakness, malicious software attack and other security related incidents or weaknesses must be reported. The MOD is a contributing Department to the Government wide Unified Incident and Reporting Scheme (UNIRAS). The rules for incident handling are covered in **Chapter 11**.

Compliance

01110. The achievement of Accreditation for a system declares that an Accreditor, as a Competent Authority has reviewed and accepted the Risks and their Management for the system(s) as installed. The validity of this situation can only endure as long as the Risks do not change, and the configuration is unchanged.

01111. To maintain effective security for the lifetime of a system, in addition to the measures inherent in Project Management structures such as Security Working Groups (SWG) and Configuration Management (CM) Boards, additional procedures are required that ensure ongoing compliance with security requirements until the system is finally withdrawn.

01112. Any system used to store, process or forward Official Information may be subject to technical or procedural Compliancy review by appropriate MOD Security Authority staffs, or other Competent Bodies agreeable to MOD Security Authorities.

01113. All Compliancy activities result in some form of deliverable, typically a report, being generated for use by the Accreditor(s) as evidence for continuance of Accreditation. Compliance checking is covered in detail in **Chapter 12**.

Security Inspections

01114. The DSO retains the right, irrespective of any delegation, to inspect without warning any IT installation within the Defence ambit, including industry and agencies. This will in certain cases override the need for local sponsorship for a visit.

British Standard 7799

01115. BS 7799 - The Standard for Information Security Management gives guidance on best practice for managing information security and provides a list of controls required to meet the standard. The Manual of Protective Security issued by the Cabinet Office has been aligned with BS 7799. Annex F provides a cross-reference between the BS 7799 high level controls and JSP 440.

This page intentionally left blank.

ANNEX A TO

CHAPTER 1

CIS CRITICALITY LEVELS

1. Criticality Levels (CL) are used to gauge the impact of any disruption to a CIS, or exploitation of any information they contain. Their purpose is to assist in deciding where security resources can be most effectively applied.

2. While it may only be possible to assign a single CL to an entire system, it will sometimes be preferable to establish CLs for each of its constituent services and infrastructures (characterised as domains, islands, connections and causeways under the DERA Domain Based Approach).

3. There are four defined CL, which in decreasing order of impact are:

4. **Criticality Level 1 (CL1).** Systems where the impact of any disruption or exploitation of any information they contain would cause exceptionally grave damage to:

a. the planning or conduct of military operations; the effectiveness or security of UK or Allied forces,

b. the effectiveness of highly valuable security or intelligence operations,

c. relations with allies, coalition partners or friendly countries,

d. the MOD's operational or business activity,

and/or

e. lead directly to loss of life or threaten the internal stability of the UK.

5. CL1 systems will therefore be predominately those systems which are critically essential to the UK's war fighting capability (eg Command and Control, weapon platforms/systems and some communication, logistic and admin systems) and those which process and store critical and highly sensitive intelligence information.

6. **Criticality Level 2 (CL2).** Systems where the impact of any disruption or exploitation of any information they contain would cause serious damage to:

a. the planning or conduct of military operations; the effectiveness or security of UK or Allied forces,

b. the effectiveness of highly valuable security or intelligence operations,

c. relations with allies, coalition partners or friendly countries,

d. the MOD's operational or business activity,

and/or

e. threaten life directly.

7. CL2 systems will therefore be predominately those systems which directly support the UK's war fighting capability (eg operational and some logistics and admin systems, essential management and finance systems).

8. **Criticality Level 3 (CL3).** Systems where the impact of any disruption or exploitation of any information they contain would materially damage:

a. the planning or conduct of military operations; the effectiveness or security of UK or Allied forces,

b. the effectiveness of highly valuable security or intelligence operations,

c. relations with allies, coalition partners or friendly countries,

d. the MOD's operational or business activity,

9. CL3 systems will therefore predominantly be those systems which contribute to the effective running and management of the MOD.

10. **Criticality Level 4 (CL4).** All other systems.

11. The Minimum Essential Defence Information Infrastructure (MEDII), which is the Defence element of the UK Critical National Infrastructure (CNI), will consist of all CL1 systems, and the segment of those CL2 systems required at that particular time to support the following basic functions :

a. Nuclear Deterrent Forces ;

b. Current Military Operations ;

c. Current Operations in Support of :

(i) UK civilian populace ;

(ii) Defence Allies ;

(iii) Intelligence Collection.

12. **Appendix 1** provides a worksheet to assist in assessing CLs. The worksheet is designed for use with information systems, but may also be applied with care to communications and infrastructure systems. The precise CL to be assigned is a matter of judgement by the Data Owner or System Operating Authority: the worksheet is intended for guidance only but, where it is decided to assign a CL at variance from the calculated CL, the rationale for doing so should be clearly documented in the Security Policy Documentation for the CIS concerned. Advice on use of the worksheet may be obtained from the appropriate TLB Principal Security Adviser.

This page intentionally left blank.

APPENDIX 1 TO ANNEX A TO CHAPTER 1

CIS CRITICALITY LEVEL WORKSHEET TEMPLATE

(……..)
Insert Appropriate Protective Marking when complete

IDENTIFICATION OF CRITICALITY LEVELS FOR MOD CIS

1. In order to determine Criticality Level of individual MOD CIS, the following criteria should be used to provide a numerical value for each of the following questions. If the answer to any question covers more than one answer, then you should tick each answer and then add them together to calculate the overall total for each question. For a CIS decomposed into its functional elements (Services / Infrastructures or Domains / Islands / Connections / Causeways) the calculation should be done for each element.

2. Please enter the following information:

a. System Name:_____

b. System Locations:_____

c. Brief description of the system:

(……..)
Insert Appropriate Protective Marking when complete

(……..)
Insert Appropriate Protective Marking when complete

SYSTEM CORE FUNCTION/ROLE

3. Is the system employed to support any of the following Core Functions?

a.	Central Government.	10
b.	Nuclear Deterrence.	8
c.	Weapon Delivery Platform.	8
d.	Operations.	8
e.	C^4ISR	8
f.	Communications	6
g.	Intelligence.	5
h.	Training.	3
i.	Administration.	1

Range 1 – 10, Typical 8 Score _____

4. What would be the effect on any of the above Core Functions if the service provided by the system was not available?

a.	Cause the Core Function to end.	20
b.	Cause severe damage to the Core Function.	10
c.	Cause moderate damage to the Core Function.	5
d.	Cause limited damage to the Core Functions.	2
e.	Have no effect on the Core Function.	0

Range 0 – 20, Typical 5 Score _____

5. How many individuals are dependent on the functions provided by the system?

a.	Less than 10	0
b.	Between 10 and 100	5
c.	Between 100 and 250	8
d.	Between 250 and 500	10
e.	Over 500	20

Range 0 – 20, Typical 20 Score _____

System Core Function/RoleSub-Total_____

(……..)
Insert Appropriate Protective Marking when complete

(……..)
Insert Appropriate Protective Marking when complete

CONNECTIVITY

6. How many other systems is the MOD CIS connected to? Direct or indirect connection to the Internet equates to unknown number of systems.

a.	None, system is a standalone LAN.	-5
b.	One system.	1
c.	Two to five systems.	3
d.	Six to ten systems.	5
e.	Ten to twenty systems.	10
f.	Unknown number of systems.	20

Range minus 5 – 20, Typical 3 Score _____

7. Is the system reliant on **any** other system for the transmission or receipt of data to fulfil its Core Function/Role?

a.	Yes.	10
b.	No.	0

Range 0 – 10, Typical 10 Score _____

Connectivity Sub-Total_____

COMMAND LEVEL

8. At what level of Defence Command will the system operate at?

Government Level	Strategic Level	Command Level	Theatre Level	Tactical Level	Non-Operational
10	10	10	10	10	0

Where a system spans more than one of the above levels, each of the values are added together, to calculate the overall score.

Score _____

Command Level Sub-Total_____

(……..)
Insert Appropriate Protective Marking when complete

(……..)
Insert Appropriate Protective Marking when complete

SENSITIVITY OF DATA PROCESSED

9. What is the highest Protective Marking level the system will operate at?

a.	TOP SECRET .	10
b.	SECRET.	7
c.	CONFIDENTIAL.	5
d.	RESTRICTED.	1
e.	UNCLASSIFIED.	-5

Range minus 5 – 10, Typical 7 Score _____

10. Does the system process any of the following Caveats?

a. STRAP 1 or 2.
b. Compartmented Information.
c. VRK.
d. COSMIC, ATOMIC or ATOMAL.

(1)	Yes.	10
(2)	No	0

Range 0 –10, Typical 0 Score _____

Sensitivity of Data Sub-Total_____

AVAILABILITY

11. Will the system be required during:

a.	Peace, Crisis and full scale War.	10
b.	Peace and periods of Crisis	5
c.	Only peacetime	0

Range 0 – 10, Typical 10 Score _____

(……..)
Insert Appropriate Protective Marking when complete

(……..)
Insert Appropriate Protective Marking when complete

12. What availability scale is required for the complete system?

a.	Full availability at all times.	10
b.	Full availability during any specific time period.	10
c.	99% availability in any given 24hr period.	8
d.	90 to 98% availability in any given 24hr period.	6
e.	75 to 89% availability in any given 24hr period.	4
f.	Less than 75% availability in any given period.	0

Range 0 – 10, Typical 6 Score _____

13. During what phases of any crisis, conflict or war will the system be required to support?

a.	Full duration of any operation.	10
b.	Only required to support weapon platforms during conflict.	8
c.	During operational planning.	6
d.	During initial preparation phase of an operation.	4
e.	Recovery from a deployed operation.	2
f.	Not required to support any deployed operation.	0

Range 0 – 10, Typical 10 Score _____

14. What is the acceptable timeframe for the system not being available to users?

a.	Less than 30 minutes.	10
b.	Less than 1 hour.	8
c.	Less than 6 hours.	6
d.	Less than 12 hours.	4
e.	Over 12 hours.	0

Range 0 – 10, Typical 2 Score _____

(……..)
Insert Appropriate Protective Marking when complete

(……..)
Insert Appropriate Protective Marking when complete

15. Can the function of the system be replicated by other means within an acceptable operational outage time and within resources likely to be available?

a.	No.	10
b.	Partially.	0
c.	Yes.	-10

Range minus 10 – 10, Typical 0 Score _____

16. List those applications which support the Core Function of the system. and give the appropriate value. If there are more than 10 such applications, the most significant 10 should be chosen. Score is the highest ***single*** value achieved by any of the applications.

a.	Full availability at all times.	10
b.	Full availability during any specific time period.	10
c.	99% availability in any given 24hr period.	8
d.	90 to 98% availability in any given 24hr period.	6
e.	75 to 89% availability in any given period.	4
f.	Less than 75 % availability in any given period.	0

APPLICATION	VALUE

Score _____

Availability Sub-Total_____

(……..)
Insert Appropriate Protective Marking when complete

(……..)
Insert Appropriate Protective Marking when complete

INTEGRITY

17. What is the level of Integrity is required for the system?

a.	Full Integrity will be required.	10
b.	Acceptable small number of inaccuracies of data.	5
c.	Integrity of the information is not critical.	0

Range 0 – 10, Typical10 Score _____

18. What would be the effect on the complete loss of the system?

a.	Cause any operation to end.	10
b.	Cause severe damage to any operation.	5
c.	Cause moderate damage to any operation.	2
d.	Cause limited damage to any operation.	1
e.	Have no effect on any operation.	0

Range 0 – 10, Typical 2 Score _____

Integrity Sub-Total_____

(……..)
Insert Appropriate Protective Marking when complete

(……..)
Insert Appropriate Protective Marking when complete

CRITICALITY LEVEL ASSESSMENT

19. Insert the appropriate **Sub-Totals**:

a.	**System Core Function/Role .**	_____
b.	**Connectivity.**	_____
a.	**Command.**	_____
b.	**Sensitivity of Data Processed.**	_____
c.	**Availability.**	_____
d.	**Integrity.**	_____

Overall Score _____

Criticality Level 1 Value	170+
Criticality Level 2 Value	110 to 170
Criticality Level 3 Value	50 to 110
Criticality Level 4 Value	Below 50

20. Criticality Level for_____System is_____

(……..)
Insert Appropriate Protective Marking when complete

ANNEX B TO

CHAPTER 1

GENERAL POLICY RELEASE OF INFORMATION ABOUT CIS SECURITY PRACTICES WITHIN MOD

DEFENCE ADVISORY NOTICES ISSUED BY THE DEFENCE, PRESS AND BROADCASTING ADVISORY COMMITTEE BEING A VOLUNTARY CODE WHICH PROVIDES ADVICE TO THE MEDIA ON ISSUES OF UK NATIONAL SECURITY

1. Public discussion of the United Kingdom's defence and counter-terrorist policy and overall strategy does not impose a threat to national security and is welcomed by Government. It is important, however, that such discussion should not disclose details which could damage UK national security. The Defence Advisory Notice System is a means of providing advice and guidance to the UK media about defence and counter-terrorist information, the publication of which would be damaging to the UK's national security. The system is voluntary, it has no legal authority and the final responsibility for deciding whether or not to publish rests solely with the editor or publisher concerned.

2. DA Notices (formerly D-Notices) are issued by the Defence, Press and Broadcasting Advisory Committee (DPBAC), an advisory body composed of senior civil servants and editors from national and regional newspapers, periodicals, news agencies, television and radio. (Membership of the Committee is given on pages 8 and 9). It operates on the shared belief that there is a continuing need for a system of guidance and advice such as the DA Notice System, and that a voluntary, advisory basis is best for such a system.

3. The current edition of the DA Notices was issued in 1993 and recognises the changed circumstances following the break- up of the Soviet Union and Warsaw Pact and the UK's involvement in smaller-scale conflicts, the undiminished threat from terrorist attacks and the risk of proliferation of weapons of mass destruction. It also takes account of the continued targeting of the UK by foreign intelligence services.

4. Compliance with the DA Notice system does not relieve the editor of responsibilities under the Official Secrets Acts.

5. The Secretary DPBAC (the DA Notice Secretary) is the servant of the Government and the Press and Broadcasting sides of the Committee. He is available at all times to Government departments and the media to give advice on the system and, after consultation with Government departments as appropriate, to help in assessing

the relevance of a DA Notice to particular circumstances. Within this system, all discussions with editors, publishers and programme makers are conducted in confidence.

6. The DA Notice Secretary may be contacted at Ministry of Defence, Northumberland House, Northumberland Avenue, London SW2N 5BP.

DA NOTICE NO 4

CIPHERS AND SECURE COMMUNICATIONS

1. It is requested that no details be published, without prior consultation, of HM Government's highly classified codes and ciphers, ***related data protection measures*** and communication facilities, or those of NATO or other allies.

2. It is also requested that advice be sought before disclosing, or elaboration on, information published at home or overseas about UK official codes and ciphers or their potential vulnerability.

3. Rationale. Disclosures that could compromise codes and ciphers put at risk the classified information protected by them. ***Revealing details of associated data protection measures*** and communications facilities, ***whether obtained, for example, from documents or by techniques such as computer hacking, could assist potential enemies to penetrate these elements of national security.***

ANNEX C TO

CHAPTER 1

THE PROTECTION OF INFORMATION HELD ON IT SYSTEMS

General Principles

1. The protection of information is covered in some detail in other volumes of the Defence Manual of Security; the purpose of this Annex is to consider some of the implications, particularly when information is held on IT systems.

2. a. In general terms, all information has some value whether that represents the value of resources spent on its collection and recording or the value that can be gained from its exploitation. When assessing its value a judgement has to be made on the degree of damage likely to be caused to government assets caused by **compromise**. The cause of compromise can be broken down into four general groups:

(1) Disclosure.

(2) Theft.

(3) Destruction.

(4) Tampering.

b. Based on an assessment of the outcome of such a compromise all assets, whether information or physical items are allocated a **Protective Marking**. A table setting out these criteria is at Appendix 1 to this Annex.

c. Also, in general terms, information can be owned and the owner can and should be responsible for determining its level of protection (see paragraph 5 below). This includes information released to the UK Government by international agreement or on a commercial basis.

3. Information concerned with the business of Government or Service activities, which a Crown Servant or a Government contractor has by his or her position as such, is deemed to be "official" and the communication of any "official" information to any person (other than one authorised to receive it) is expressly forbidden by the Official

Secrets Act. The originator of "official" information is not, therefore, the owner of that information. The rules for the protection of "official" information are based on the allocation of a protective marking, the criteria for which are set out in other security publications. The authority to allocate a protective marking is limited to certain ranks and appointments, although in an emergency the originator of a document of any rank may authorize any protective marking provided the definitions laid down are used and can be justified.

National Caveats

4. Instructions for the use of national caveats are promulgated in other security publications but some important extracts are set out here with regard to the two core national caveats.

a. **UK EYES ONLY.** Information bearing the national caveat UK EYES ONLY is not to be released to any other country and, within UK Government Service, is strictly to be confined to those staff as detailed in JSP 440 Volume 1. It should be used sparingly. Originators are reminded that indiscriminate use can lead to transmission and custody difficulties and it should only be used where there is a real risk that information, whose uncontrolled disclosure would cause real damage to the UK, may inadvertently or unwittingly be disclosed to those who are outside the listed categories. It should not be used where the originator wishes to indicate that information is not to be released to a particular country. In such cases this should be indicated in the text eg "This information is not to be passed to the Ruritanians"

b. **UK EYES DISCRETION.** Information bearing the national caveat UK EYES DISCRETION is not to be released to any other country, nor to any other than a person in the above category or, on a discretionary basis to a slightly wider category listed in JSP 440 Volume 1. Information may be released by originators or owners of the information only to those detailed in Chapter 16 of Volume 1. In marking material with this caveat, the originator is delegating his release authority (including that of the PROTECTIVE MARKING) to the named recipient(s) (ie a named individual or specific post). It may, therefore, at the named recipient's discretion, be released to other UK and dual nationals (provided one nationality is British) and exchange/integrated officers and officers on attachment to UK Armed Forces, only where the conditions detailed in Chapter 16 of Volume 1 are met. It thus provides flexibility for named recipients to make a valued judgement on further dissemination, immediately, and without reference to the originator of the information but having regard to the release of information table in JSP 440 Volume 1 Chapter 11.

Mandatory Protective Marking Levels

5. In some cases, information on a particular subject will attract a mandatory protective marking. Mandatory degrees of protection are also associated with projects covered by codewords of various kinds and statistical records. In these cases the originator of an item of information may not protectively mark it lower than the mandatory prescribed level. In Information Technology (IT) terms, the degree of protection is "owned" by the authority setting the mandatory level and the originator is the "holder" of that protective marking. This is an extension to the existing rule in other security documentation whereby holders of documents protectively marked CONFIDENTIAL and all documents protectively marked SECRET or higher have to consult the originator if they consider a regrading is necessary.

Aggregation of Information

6. The sensitivity of information is greatly influenced by the context in which it is, or can be viewed. The aggregation of information and its exploitation by electronic processing is the basis of the IT revolution. The security of a set of information may attract a higher degree of protection than an individual record and the originator of a piece of information may be unaware of its ultimate sensitivities. For instance the reliability of a fleet of vehicles is of higher sensitivity than for a single vehicle. If that fleet could be more closely defined as essential to an operational theatre, then it would be higher still. The IT System Manager, acting on behalf of his command authority, may need to take advice on the degree of protection necessary for such aggregated information and to assign a higher mandatory level to a computer document after processing. There may also be a need to anticipate an overall degree of protection for the IT system which allows for aggregation of user data. This may be particularly important when considering the level of compromise which might result from the destruction or tampering of a database. In some cases it may be possible to employ the opposite effect of decreasing the security application of information by removing the appropriate context, such as is used in "veiled" speech.

This page intentionally left blank

ANNEX D TO CHAPTER 1

PROTECTION OF COMPARTMENTED INFORMATION

Overview

1. For some categories of sensitive material or externally sourced material, generically referred to as Compartmented Information, but often referred to as Codeword material, in addition to the general requirements for system and site Accreditation from the designated Accreditor(s), approval is also required from all relevant Control or Release Authorities before the material may be stored, processed or forwarded on the system(s).

Compartment Approval

2. Compartment Approval may be referred to by 3rd parties (i.e. those outside MOD) as an "Accreditation", but within MOD the term Accreditation is reserved for the activity of ensuring that the systems is implemented to meet the needs of UK protectively marked material at the High Water Mark of any and all compartments to be used, which is carried out by the PSyA or their nominated representative.

Risk Assessment

3. The only Compartmented Information which has a MOD recognised Risk Assessment methodology is the STRAP system as laid down in JSP440 Volume 5. In order to assess the overall security requirements for other Compartmented data, a STRAP Equivalent Level (SEL) should be derived before discussing protection requirement with Security staffs. Advice on the selection of an appropriate SEL can be obtained from D Def Sy.

Compartment INFOSEC Representative

4. Where the Compartmented Information has a formal Control or Release Authority, a Designated Security Authority (DSA) or Cognizant Security Authority (CSA) will normally fulfil the capacity of a Compartment Infosec Representative (CIR) for the material concerned, acting as a Competent Authority on behalf of the Control / Release Authority.

5. In the cases of Compartmented Information where the UK Control or Release Authority resides within MOD, for instance the ATOMIC system, the DSA must be

drawn from the staff of one of the MOD Accreditation Authorities. The Control / Release Authority is responsible for nominating their CIR(s), and the details of this nomination must be supplied to D Def Sy in accordance with the format laid down at Appendix 1. In selecting an Agent, the following metric should be used :

a. Where the system(s) processing the Compartmented Information are solely contained within the real estate of a single PSyA, that Authority should be asked to acts as the CIR;

b. Where the system(s) processing the Compartmented Information cross Authority boundaries, either within or without MOD, including NATO or Other Government Departments (OGD), D Def Sy should be consulted, and may in some cases elect to nominate a D Def Sy staff officer to fill this capacity.

6. Compartmented Information not solely controlled within MOD, for instance STRAP, will have their own arrangements for appointment of CIRs, and any queries should be addressed to D Def Sy.

7. Where a requirement to process information from a compartment is identified, but the CIR is not known to the project office, then D Def Sy should be consulted.

Incident Handling

8. If any security incident occurs affecting systems used to store, process or forward Compartmented material, then in addition to any local reporting arrangements, the MOD Joint Security Co-ordination Centre, which has overall responsibility for such matters on behalf of the Departmental Security Officer, must also be informed immediately. JSyCC can be contacted on 020-7218-4505 (84505MB).

APPENDIX 1 TO ANNEX D TO CHAPTER 1

FORMAT FOR NOMINATION OF COMPARTMENT INFOSEC REPRESENTATIVE (CIR)

(……..)

Insert Appropriate Protective Mark when complete

Compartment Reference Number[1]			
	Name		**Protective Marking**
Common Name or CodeWord			
Other Codewords[2]			
Short UNCLASSIFIED Description[3]			
Compartment Overview	**Details**		**Protective Marking**
STRAP Equivalent Level (Protection Required)[4]			
	Post	**Location**	**Telephone**
Compartment Controller			
Compartment Infosec Representative Nominee			

Notes

1 To be supplied by DDefSy

2 List

3 If no existing UNCLASSIFIED description exist, a simple statement such as "Special Intelligence" should be used.

4 Details as to SEL derivation from DDefSy

Insert Appropriate Protective Mark when complete

(……..)

This page intentionally left blank

ANNEX E TO

CHAPTER 1

SECURITY INSTRUCTIONS FOR HOMEWORKERS INVOLVED IN THE HANDLING OF OFFICIAL MATERIAL

Introduction

1. These instructions are designed to ensure that the minimum standards which protect information in MOD offices are applied, as far as possible, in home circumstances and a copy will accompany all letters of appointment for Homeworkers. They may not be relaxed and may be applied only in Great Britain. These rules will also apply to those MOD office-based employees who regularly take work home.

General

2. Homeworkers are now permitted to have access to official material with a protective marking up to and including RESTRICTED, provided:

a. He or she understands his/her obligations in respect of the physical and procedural security measures necessary to protect such material; and

b. All the necessary practical arrangements, as called for by security staffs, have been made to ensure they can be fulfilled.

3. Before homeworking commences the homeworker must provide his or her line manager with written agreement to a visit to the home (and, thereafter, to periodic spot checks) by representatives of the security directorate to confirm that satisfactory physical and procedural security measures are in place. Such agreement must be confirmed whenever regular access to official material is involved, irrespective of protective marking level.

Personal security

4. Homeworkers should be especially careful not to draw attention to the fact that they are working on official information at home. As homeworkers will have few opportunities to discuss work or problems with colleagues, they may be more vulnerable to compromise by someone professing to show an interest in their work. They need to

be alert to this danger and instances of outsiders (or those without a `need to know') showing undue interest should be reported to the Departmental Security Officer.

Security in the Workroom/Work Area (including Storage of Material)

5. Many aspects of security which are taken for granted in MOD buildings and establishments are difficult to replicate in the home. As far as is possible, homeworkers must adhere to the following guidelines:

a. Where possible, a lockable room should be set aside as a working area, used exclusively for official work. If this is not possible, a working area should be selected to minimize, and control, unexpected interruptions from family or visitors.

b. If interruptions occur during official work, the homeworker should ensure that official papers, and particularly protectively marked papers, are covered so that they cannot be overlooked.

c. When not working on it, official material should be stored in an appropriate locked container (the key(s) to which must be held personally by the homeworker), unless:

(1) The homeworker intends to return to it after a short interval: and

(2) It is in a room to which the door and windows have been locked; and

(3) The homeworker remains in the home.

Connection to Departmental Computer Systems

6. Connection to other departmental computer systems from the home premises may be permissible subject to approval from the appropriate security authority and that the following additional security requirements are met:

a. The highest protective marking of material which may be held or processed on the homeworker's computer system and any connected departmental computer system is RESTRICTED.

b. The official computer to be used in the home premises must have an approved access control mechanism implemented. This may be as an inherent part of the Operating System or as an additional hardware/software package.

c. The communications link between the home and the departmental computer must be protected by encryption to an approved government standard.

d. The official computer to be used in the home premises must not be connected to any non-departmental system.

e. All IT equipment to be used for official purposes in the home must have approved SyOPs (see Appendix 1).

f. Approval for connection from the official computer in the home to departmental computer systems must be granted by the appropriate security authority on an individual case by case basis.

Telephone Security

7. Homeworkers should be alert to the dangers of passing protectively marked material, or information of possible use to terrorists for targeting purposes, over the public telephone network. Always confirm the identity of originators/recipients of telephone calls. To minimize risk of eavesdropping, party-lines or multi-extensions are not advisable. Similarly, use of radio telephones (including cordless and cellular telephones) for passing RESTRICTED material is prohibited. The following table addresses the precautions necessary when using the telephone to discuss classified or privacy-marked information:

Type of Telephone Call			
	Within Mainland UK Excluding Northern Ireland	To & Within Northern Ireland	Overseas
Protective Marking	RESTRICTED	UNCLASSIFIED	UNCLASSIFIED

Facsimile Transmission Security

8. The considerations outlined in the previous paragraph also apply to facsimile transmissions. Where the need for speed is paramount an officially approved facsimile machine located in the home may be used for passing material protectively marked up to and including RESTRICTED over networks within the UK. The homeworker must verify that the recipient is ready to receive the message prior to transmission. Unprotected circuits outside the UK and to Northern Ireland are only to be used to transmit UNCLASSIFIED information.

Computer and Word Processor Security

9. All IT equipment to be used for official purposes by the homeworker must be approved by the appropriate security authority prior to installation. Equipment featuring integral disks or non-volatile memory (which is not erased when the mains power is switched off) is not be used.

10. All information and programs must be must be protected in accordance with the policy for portable CIS in **Chapter 8**. All removable disks should be secured under lock and key (see para 5a).

11. To avoid the possible danger of introducing malicious software, the following additional requirements must be met:

a. Only disks supplied by the Department should be used.

b. The equipment should be used solely for official purposes.

c. Official disks should not be used for personal matters.

d. Disks used for protectively marked information should carry a label showing RESTRICTED.

e. Disks should carry a unique serial number.

f. When, for whatever reason, a disk becomes unusable or surplus to requirements, it should be returned to the Department for disposal/destruction.

g. 'On-access' virus protection software must be installed and active at all times. The installed anti-virus software must be updated on a regular (monthly or better) basis. If the home base employs 'boundary virus protection', all disks used on the portable system must be treated in the same way as a systems in an external organization.

Photocopying/Printing

12. It is important to keep copies of documents to the minimum necessary for the proper conduct of business. Reproduction of RESTRICTED documents should be undertaken on an approved photocopier supplied by the Department for the purpose, or on a machine available within the Department itself. UNCLASSIFIED material may be reproduced on local commercial copiers if operated by the homeworker, care being taken to ensure as far as possible that documents are not read, or identified as MOD/official material by others. RESTRICTED and above material may only be printed on an approved photocopier or printer supplied by the Department for this purpose, or an a machine available within the Department itself.

Posting of Documents and other Material to, from and between Homeworkers

13. The minimum standards for transmitting documents and other material through postal services are as follows:

Protective Marking	Enveloping, sealing, marking	Approved means
RESTRICTED	Single envelope. No post	Ordinary letter
RESTRICTED + Descriptor	As above + Address by name and mark Personal for	As above
UNCLASSIFIED	Single envelope	As above

14. The homeworker's attention is drawn to:

a. Postal arrangements for Northern Ireland and the Republic of Ireland; and

b. The use of return addresses on official mail.

Carriage - by the Homeworker and other Departmental Staff

15. Where it is necessary to remove RESTRICTED material from the home (to attend a meeting, for example), it should be carried in a locked container such as a briefcase. The container is to bear a label securely attached to the outside giving instructions to the finder. Only one side should normally be visible, the reverse being obscured by a protective cover. The visible side of the label is to read: `If found please see instructions on the reverse side of this label'. The reverse side is to read: `Anyone finding this [container] is asked to telephone 01371-854444 or hand it in at the nearest police station or railway or other transport authority with a request that they should take that action'.

Note: The telephone number given is that of the Security Control Room in Main Building. The number of the appropriate Service security authority may be given instead.

16. While carrying protectively marked documents, the container should remain at all times in the homeworker's personal possession. Protectively marked documents should not be read in any public place or public vehicle. Note: Never journey abroad or to Northern Ireland carrying a briefcase bearing the Royal cypher.

Review of Holdings

17. The homeworker should minimize official material held at home. Holdings should be reviewed at least every six months and, where appropriate, forwarded/returned to the Department.

Destruction of Waste

18. UNCLASSIFIED paper waste may be disposed of by shredding or tearing it into small pieces and placing into household waste bins; it must be well mixed with domestic rubbish. RESTRICTED papers must be disposed of by a method approved by the appropriate security authority or returned to the Department for secure disposal. Non-paper waste must always be returned to the Department for secure disposal.

Files

19. MOD practice should be followed. This normally means that documents should be filed, in date order, as soon as possible and a file minute sheet kept.

File Lists

20. Lists of all files held at home should be kept by both the Department and the homeworker.

APPENDIX 1 TO

ANNEX E TO

CHAPTER 1

GENERIC SYOPS FOR COMPUTERS USED FOR HOMEWORKING

Introduction

1. This document constitutes the Security Operating Procedures (SyOPs) for the IT system, detailed below, to be used for homeworking. They are issued by the ITSO in accordance with Defence Manual of Security Volume 3, and have been approved by the Accreditor. All personnel using the system are to comply with these SyOPs, and no departure from or amendment to them is permitted unless prior authorization is obtained from the Accreditor.

2. Breaches of these orders may render the offender liable to disciplinary action.

Equipment Details

3. The equipment covered by these SyOPs is:

Make:

Model:

Serial No:

Administration

4. The ITSO for this system is:

Job Title:

Branch:

Tel No:

5. The ESyO for this system is:

Job Title:

Branch:
Tel No:

6. Authorized users of this system are listed at ANNEX A. Additions, deletions and amendments to the list of authorized users must be approved by the ITSO.

7. The highest protective marking of material which may be held or processed on this system is: RESTRICTED.

Personnel Security

8. All authorized users of this system must have the appropriate security clearance for the material processed on the system.

Personal Security

9. Homeworkers should be especially careful not to draw attention to the fact that they are working on official information at home. Instances of outsiders (or those without a 'need to know') showing undue interest should be reported to the Departmental Security Officer.

Security in the Workroom/Work Area (including Storage of Material)

10. Many aspects of security which are taken for granted in MOD buildings and establishments are difficult to replicate in the home. As far as is possible, homeworkers must adhere to the following guidelines.

a. Where possible, a lockable room should be set aside as a working area, used exclusively for official work. If this is not possible, a working area should be selected to minimize, and control, unexpected interruptions from family and visitors.

b. If interruptions occur during official work, the homeworker should ensure that, as a minimum, the computer screen is cleared so it cannot be overlooked although activation of the access control mechanism is preferred.

c. When not working on it, official material should be stored in an appropriate lockable container (the key(s) to which must be held personally by the homeworker) unless:

(1) The homeworker intends to return to it after a short interval: and

(2) It is in a room to which the door and windows have been locked: and

(3) The homeworker remains in the home.

(4) Under no circumstances should the homeworker's computer be left unattended without the communications link to the department's computer system being disconnected and the access control mechanism activated.

Physical Security

11. The system is normally based in:

12. Where the system is normally based on an MOD site but transported to and from home premises On a regular basis, blanket permission, covering a suitable period of time, must be obtained from the ESyO or ITSO for this type of removal.

13. Where the system is to be based at the home premises, permission for this type of usage must be obtained from the ESyO or ITSO.

14. In addition to the above a register must be maintained showing occurrences of removal of the system from the MOD site. This register should show the date of removal, responsible officer, location system taken to, and the date the equipment was returned.

15. When not in use the system and any associated magnetic media, eg floppy disks, removable hard disks, etc, must be protected and handled in a manner commensurate with the highest protective marking of material processed on the system.

16. While equipment and any associated removable media are in transit outside a secure MOD environment, the media, where possible, should be carried separately from the equipment. In addition, where a portable computer incorporates a rechargeable battery pack, this must be removed or disconnected to allow internal memory to discharge. All IT equipment to be used for official purposes by the homeworker must be approved by the appropriate security authority.

17. All information and programs must be protected in accordance with the policy for portable CIS in **Chapter 8**. All removable disks should be secured under lock and key.

18. To avoid the possible danger of introducing malicious software, the following additional requirements must be met:

a. Only disks supplied by the Department are to be used.

b. The equipment must only be used for official purposes.

c. Official disks are not to be used for personal matters

d. Disks used for protectively marked information are to carry a label showing RESTRICTED.

e. Disks must be marked with a unique serial number.

f. When, for whatever reason, a disk becomes unusable or surplus to requirements, it is to be returned to the Department for disposal/destruction.

19. Connection of the computer used at the home premises is strictly limited to those departmental IT systems and equipments to which the homeworker would connect in the course of their duties when at the MOD site. Remote connection to these IT systems is only permissible using encryption to an approved government standard over the communications link. Under no circumstances may the computer used by the homeworker be connected to any other computer system or network.

Hardware Security

20. Equipment must be checked before use for obvious signs of tampering. Any suspected problems should be reported to the ITSO without delay and the equipment should not be used until checked and cleared.

Software Security

21. No software from unauthorized sources may be loaded into the system.

22. Back-up copies should be made of any software or data essential to the operation of the system. These should be kept in a different location to the working copies of the software and data flies. Back-up copies should be made frequently and an annual test should be conducted to verify the back-up copies are usable.

23. Individual users are responsible for ensuring that back-up copies of any data files essential to their work are adequately maintained.

24. Any suspected attack by virus or other malicious software must be reported to the appropriate security authority without delay and the system must not be used until a security investigation has been carried out.

ANNEX A

LIST OF AUTHORIZED USERS

Name	Designation	Official Address	Tel	SyOPs Read	
				Date	Signature

This page intentionally left blank.

ANNEX F TO

CHAPTER 1

CONTROLS FOR INFORMATION SECURITY MANAGEMENT

(From British Standard (Bs) 7799 "Code Of Practice For Information Security Management")

High Level Controls

BS7799 Part I Control	JSP 440 Reference
3. Security Policy	JSP 440 Volume 1 Chapter 1. JSP 440 Volume 3 Chapters 1 and 2
4. Security Organisation	JSP 440 Volume 1 Chapter 2. JSP 440 Volume 3 Chapter 2
5. Asset Classification and control	JSP 440 Volume 1 Chapter 1 and Chapter 4. JSP 440 Volume 3 Chapter 14
6. Personnel Security	JSP 440 Volume 2. JSP 440 Volume 3 Chapter 11
7. Physical and Environmental Security	JSP 440 Volume 1 Chapter 5. JSP 440 Volume 3 Chapters 2 and 4
8. Communications & Operations Management	JSP 440 Volume 3 Chapters 2, 4, 6, 7, 17, 24, 25 and 26
9. Access Control	JSP 440 Volume 3 Chapters 2, and 6
10. Systems Development and Maintenance	JSP 440 Volume 3 Chapters 2, 3, 6 and 23
11. Business Continuity Management	JSP 440 Volume 3 Chapter 1 and MOD Guide to Business Continuity
12. Compliance	JSP 440 Volume 3 Chapters 1, 11 and 12

Notes:

1. JSP 440 Chapter 11 is referenced against BS 7799 Part I Control 6 Personnel Security since this is where BS 7799 places Incident handling.

This page intentionally left blank

ORGANISATION AND MANAGEMENT OF SECURITY

CHAPTER 2

ORGANISATION AND MANAGEMENT OF SECURITY

Introduction

02001. This Chapter gives guidance on the Organisation and Management of for Communications and Information Systems (CIS) in use within Defence. It is a principle that the security approval and compliance functions should be separated, wherever possible, from the project management and the system operating authority functions and should reside under a separate chain of command.

02002. A requirement for good management practices applies throughout the system lifecycle:

a. Inception

b. Implementation

c. Operation

d. Decommissioning

02003. However, for routine systems, the emphasis is on the security management activities in the Operation phase. More detail on security requirements for other phases, applicable normally to large and complex systems, can be found at Chapter 13.

02004. Within the Operation Phase, the following Security Management Activities are required:

a. System Security Management;

b. Security Accreditation;

c. Security Compliance.

Organisation of Security within Defence

02005. Departmental Security Officer (DSO). The DSO, the Director General Security &Safety (DGS&S) is responsible for Security policy in Defence and for ensuring that the minimum standards for IT Security laid down by the Government are applied.

02006. Directorate Defence Security (D Def Sy). D Def Sy leads in the protective and procedural policy area, supported with technical advice on standards, practices and interpretation of procedures from EC-CCII-IOCM staff.

02007. In order to provide effective and efficient security policy for MOD information and communications systems, the staffs of D Def Sy on behalf of the Departmental Security Officer, and CM(IS) co-operate at every level. Coordination of policy is achieved by cross representation on security policy and technical security policy committees and working groups.

02008. Interim policy is issued in a number of different ways, depending on the perceived needs:

a. Widely applicable Policy of general relevance is issued by DCIs prepared by the Infosec Policy Working Group;

b. More specialist Technical Security Policy is issued as Defence Information Assurance Notices (DIAN) to CIS security staffs and other interested parties, for onward dissemination as required.

02009. Where appropriate this guidance is submitted for inclusion in later versions of JSP 440, and it can be assumed that any DCI, which was issued more than 3 months before the publication date of the latest update to this volume has been superseded. UNCLASSIFIED DIANs will normally be available on the MODWEB and similar Intranets, and on the Security Section of the MOD ICS catalogue CD-ROM.

02010. Defence Security Standards Organisation (DSSO). The DSSO task falls into two main areas:

a. provision of a centralised CIS security accreditation service for the major Communications and Information Systems in MOD;

b. provision of an independent security audit capability to enable the DSO to certify that security policy is being implemented adequately and cost-effectively across the whole of MOD and its Trading Funds.

02011. DSSO accreditors will advise business managers of the risks to their CIS systems and how best to mitigate and reduce them. The decision to accept the residual risk will lie with the business manager in consultation with other stakeholders. DSSO auditors will focus on assessing the effectiveness of the integrated risk management process of the TLB Holder/Trading Fund Chief Executive (TFCE).

02012. Top Level Budget Holders (TLBs) and Trading Fund Chief Executives (TFCEs). Responsibility for the implementation and risk management of security policy and standards has now been formally delegated to TLB Holders/TFCE. Each

TLB Holder/TFCE is required to nominate a Security Risk Manager to advise the TLB/TFCE on the balance between business needs and security requirements, taking account of affordability, and act as a TLB/TFCE point of contact with the DSO.

02013. Principal Security Advisers (PSyAs). A PSyA is appointed by each TLB Holder and TFCE. The services of another TLB may be chosen to provide the relevant security advice but the responsibility and accountability for the application and maintenance of security in their area is vested in the TLB Holder/TFCE. The PSyA provides advice to the TLB Holder/TFCE and the Management Board on all security issues that have a corporate bearing on TLB/Trading Fund business. This includes undertaking a range of tasks associated with those CIS that are specific to the TLB/Trading Fund, including accreditation, of those CIS for which the TLB has been delegated responsibility, ensuring compliance with security requirements, and reporting CIS security incidents.

02014. Joint Security Coordination Centre (JSyCC). The JSyCC, which is part of the DSO's organisation, acts as the coordinating point for Security Alerting, Reporting, and Response. The JSyCC also has responsibility for management of compliance activities. The role of the JSyCC is covered in greater detail at paragraph **02045**.

Accreditation Authorities

02015. Enforcement of Security for CIS is primarily carried out by the process of Accreditation, which must be obtained before any CIS system is permitted to store, process or forward any official information. The Accreditation confirms, for the Data Owner(s), the fact that Confidentiality provisions of the implementation do not present an unacceptable risk to the Information being processed, and also confirms, for the System Operating Authority (SOA), that appropriate asset protection for Integrity and Availability is in place.

02016. Within the MOD, an Accreditor is a Competent Authority as recognised by either the DSO and/or the DSSO, tasked with performing CIS Accreditation, and must be a member of MOD staff.

02017. This role may be further delegated by the nominated PSyAs to Security staffs under their control, as required, and such staff must not have any responsibilities in respect of the operation of any systems they accredit.

02018. However, such delegation may not be given in respect of:

a. Systems used to store, process, or forward TOP SECRET material;

b. Systems used to store, process, or forward Compartmented ("Codeword" e.g. STRAP) material;

c. Systems used to store, process, or forward IDO owned material (e.g. NATO);

d. Systems defined as being Criticality Level 1 (CL1) ;

e. Systems crossing TLB boundaries;

f. Systems directly connecting outside of MOD boundaries (e.g. to Allies or OGD).

02019. It should be noted that the delegation of Accreditation Authority defined above refers solely to MOD owned material without specific Control or Release regulations. For systems storing, processing or forwarding such material, **Chapter 1 Annex D**, which deals with the Protection of Compartmented Information, must be followed **in addition to** the general security requirements laid down for all MOD CIS.

Delegated Responsibilities

02020. Normally PSyAs will be responsible for systems for which the "Data Owner" is one of their respective TLB holders or for which the TLB is financially responsible.

02021. PSyAs are responsible for maintaining a register of every IT system in their area of responsibility and for recording the level of security protective marking of data which each is authorized to process. PSyAs are responsible for notifying the Coordinating Installation Design Authority (CIDA) of the planned installation of any IT system. PSyAs are to arrange for protective security surveys and inspections of all units with systems. In addition, they are to ensure that units proposing new systems, which are likely to process data protectively marked CONFIDENTIAL or above, are also surveyed and inspected before processing is authorized. They are responsible for investigating and advising on each new proposal for a system and for ensuring that the security factors are identified and taken into account during the planning stage.

02022. Security Units. The following general delegations should be noted:

a. **Deployed Forces**. All forces deployed under PJHQ OPCOM should report security concerns to PJHQ J2(Sy) in addition to any reporting chain, which acts as the Monitoring and Reporting Centre (MRC) for incidents affecting such units, as laid down at **Chapter 11**;

b. **RN.** A Specialist RN team, DNSyICP(ITSy2), The Central Information Technology Security Section (RN), CITSS(RN), is tasked to carry out inspections of Major RN IT systems and investigate major security incidents on those systems.

c. **Army.** Intelligence Corps security units are responsible, under the direction of the security staff, for giving advice and assistance to units and headquarters on CIS security, carrying out surveys and inspections, and

investigating breaches of security. A specialist team, the Army Information Security Unit, AISU, is tasked by G2 Sy(Info). EST(A), a specialist Royal Signals unit also tasked by G2 Sy2(Info), is responsible for TEMPEST inspection in the Army;

d. **RAF.** The Regional Provost and Security Services (P&SS) unit is responsible under the direction of the relevant Security Staff for carrying out security surveys and investigating breaches of security. TEMPEST inspections are conducted by 591SU RAF Digby. Unit TEMPEST Configuration Control Officers (TCCO) are responsible for providing TEMPEST Countermeasure Assessments (TCA) in accordance with **Chapter 21**;

e. **Police (MDP and Service Police)**. Any incidents of Criminal Offences involving IT, such as theft or criminal damage, are to be reported to the Ministry of Defence Police. If the offence involves Service Personnel it should be reported to Service Police. This requirement is in addition to any involvement of Civilian Police and/or local security staffs. To meet pan-governmental security requirements for collating statistics, this nature, the incident is also to be reported using the UNIRAS scheme as detailed in **Chapter 11**.

02023. Security Investigations. Where a major security investigation is required, in accordance with **Chapter 11**, at least one member of any Investigation Team used must be aware of the requirements of the Police and Criminal Evidence Act (PACE).

02024. In the case of the Ministry of Defence Police (MDP), the Service Police, members of the Intelligence Corps or the units identified above, such knowledge can be assumed. In all other cases, staff acting as security investigators DSO. To facilitate identification, all MOD civilian staff on these duties are issued with an Investigator's Identity Card, examples of which can be obtained on request from JSyCC.

02025. Minor breaches investigations can be performed on behalf of the Head of Establishment by local Security Staffs.

System Security Management

02026. Because of the specialist knowledge required, responsibility for the security of an IT system is divided between security and user/IT staff. Amongst other things, the security staff are responsible for providing security guidance, for establishing the required security measures, and for seeking advice from the appropriate authorities. The System Manager and IT staff are responsible to the Head of Establishment or CO for the security of the system, and for selecting functions to meet the security measures required.

02027. Commanding Officers, Directors and Heads of Establishments/Divisions. Commanding Officers, Heads of Establishment/Divisions and MOD Directors have

overall responsibility for security in their units, branches or establishments. This includes IT security. They are to seek prior approval in accordance with local security instructions when submitting a case for an IT system. They are also responsible for maintaining a register of IT assets, which is to be available for inspection. See **Chapter 3**. The control of IT systems security requires careful management since normal users may lack an understanding of the technical risks involved. For that reason Unit/Establishment IT security officers (ITSOs) are to be appointed. If a large or distributed system is used within a unit then other posts may also be appointed.

02028. IT Security Officer (ITSO). In an organization as complex and as disparate as the MOD, there is no one blueprint for the organization of security, which will satisfy all systems and installations. Indeed, even within one service, the needs of differing systems may require alternative types and styles of security organization and management. The PSyA Security Staff will promulgate within their area of responsibility the detail of how security is to be organized.

02029. There is a need throughout this JSP to have a shorthand description of the organizational responsibilities at the centre of the IT spectrum of security. For convenience, these central roles have been amalgamated under the generic title of Information Technology Security Officer (ITSO). Whilst it may be possible for the person in a single post within a small system to have all such responsibilities, inevitably the individual PSyA Security Staff will decide how these responsibilities are to be split for more complex systems and at large organizations. Generic responsibilities of an ITSO are shown at **Annex A**.

02030. Additionally, the role of a Co-ordinating ITSO (CITSO) is recognised where there is a need for a ITSO, appointed under the authority of Commanding Officers / Directors / Heads of Establishments/Divisions, to have additional responsibilities for all MOD elements within a geographic area which may cut across responsibilities deriving from the security chain of command. 3 specific CITSO roles are currently recognised:

a. **Northern Ireland** HQNI G3Sy has CITSO responsibilities for all units based in, or deployed to, the Province, in addition to any security reporting chain, and acts as the Monitoring and Reporting Centre (MRC) for incidents affecting such units, as laid down at **Chapter 11**;

b. **Northern Europe** UKSC(G) G2 Sy has CISTO responsibilities for all units based in, or deployed to, Northern Europe, in addition to any security reporting chain, and acts as the MRC for such units as laid down at **Chapter 11**;

c. **North America** BDS(W) / CITSO(NA) has responsibilities for all units and all other staff based in, or deployed to, North America, in addition to any security reporting chain, and acts as the MRC for such units as laid down at **Chapter 11**.

02031. It should be noted that the term ITSO is used in other Government Departments to referred to the senior post in a Department with responsibility for IT security.

02032. System Operating Authority (SOA). All large and distributed systems, which may or may not extend outside establishment boundaries, must be operated under the Authority of an officer in whom adequate authority is delegated by the appropriate CO etc. and to whom users will be accountable. The SOA must be appointed before a system is put into service. The SOA is responsible for all aspects of system operations, but for large or complex system the day-to-day management of the system will normally be delegated to one or more System Administrators (SA) and System Security Officers (SSO). The SOA is responsible for ensuring that Security Operating Procedures (SyOPs) are both published and ensuring signed as being read and understood by all users of the system. Where the role of SOA and SA are combined, this person is normally referred to as the System Manager (SM). The responsibilities of a System Operating Authority are described at **Annex B**.

02033. System Administrator (SA). Large and distributed systems will usually be managed on a day-to-day basis by one or more System Administrators (or equivalent) to whom adequate authority is delegated by the SOA. The SA(s) should assume his duties before a system has been commissioned, and will be responsible for the extension or alteration of a system in service.

02034. Network System Security Officer (SSyO). If a SSyO is appointed, he/she should be responsible to the SOA for all aspects of the day-to-day security administration, and should have received appropriate training on the system. Where there is no SSyO, these duties will normally fall to the SOA, although it is generally desirable for these functions to be separated in all but the smallest CIS installations. The responsibilities of a SSyO are detailed at **Annex C**.

02035. Managers. When two or more systems located in separate areas are joined, there is to be a Network Manager responsible for coordinating the security arrangements; the responsibilities must be clearly defined in the Security Policy Documentation (SPD) and approved by the DSSO or appropriate PSyAs security staff. Each of the SOA will retain direct responsibility for the standard of security of his or her own system, and will be accountable to the Network Manager for meeting the security requirements of the network, as stated in the SPD.

02036. Network Security Officers (NSyOs). A NSyO is responsible for overall network security. Where all systems on a network have the same SOA (i.e. the network is managed as a single system), the SSyO may carry out this central control function. In other cases, it may be more appropriate to appoint a NSyO. Security measures to be adopted throughout the network are to be agreed between management and users and approved by the NSyO, in conjunction with the accreditor concerned, who should also be consulted concerning any proposed modification to the network or to its use. The

NSyO is to satisfy himself as to the adequacy of the network security features, including provision for:

a. Communications security.

b. Security labels (of data).

c. Access controls.

d. Audit trails.

e. Data integrity.

f. Maintenance of network security within remote terminal areas, delegating as appropriate to the respective SSyOs.

02037. Security Assurance Coordinator (SAC). For large and complex projects and systems, or sites/formations with extensive use of IT systems, a SAC should be appointed, both to provide advice and assistance to the project / system management authorities, and to reduce the resourcing implications being placed on external agencies such as Accreditors.

02038. The role of a SAC is one of the "permitted extensions" to the functions of a Project Assurance Team (PAT) as laid down within the Governmental PRINCE methodology, and can also be considered to be an expansion upon the role of an IT Security Officer (ITSO). Details of the Terms of Reference (TOR) for a SAC are laid down at **Annex D**.

02039. Installation Design Authority (IDA) and Coordinating Installation Design Authority (CIDA). No alteration or movement may be made to any system without the prior approval of the IDA/CIDA.

a. **Coordinating Installation Design Authority (CIDA).** Within the MOD, an CIDA is a Competent Authority as recognised by the DSO, tasked with ensuring that CIS equipments and systems within a site are installed in a secure manner, and must be a member of MOD staff. The CIDA is responsible for ensuring common standards of installation, and that the requirements specified for TEMPEST, EMP, EMC, Radhaz and safety are met. They will supervise and coordinate the provision of documentation for each installation. Each site with systems storing, forwarding or processing MOD information must have a designated CIDA.

b. **Installation Design Authority (IDA).** Responsible for the design of a system including the provision of installation documentation, works service specification, the specification of tests and testing procedures, and the custody and updating of master installation drawings and other relevant documentation

throughout the life of the system where there is no CIDA with this responsibility. Each system will have an IDA.

02040. Fuller details of the IDA/CIDAs and their responsibilities are shown at **Annex E**.

02041. Users. Every user of a system has a duty to ensure the security and integrity of information in the system and must understand the responsibilities for this. They must:

a. Be conversant with all security orders and instructions issued for use with the system, for which they will be required to sign confirmation;

b. Use the appropriate built-in security features of the system;

c. Ensure that all input, programs, output are allocated the appropriate protective marking and caveat. This includes all intermediate documents, which may be created during processing, and traffic to be passed over a data link;

d. Report promptly any incidents, which may have security significance, through the chain of command to the ITSO.

02042. The corollary of these responsibilities is that CIS systems are potentially more vulnerable to disaffected personnel than manual systems. Any person with access to CIS systems may be in a position to interfere with or damage the equipment and storage media; to alter or delete the data; to see or obtain sensitive material being stored, displayed, processed or otherwise handled. Particularly with office based CIS, it may be impracticable to secure such material temporarily whilst uncleared staff are working in the area without seriously disrupting the work of the unit/establishment and therefore particular care must be taken to avoid casual overlooking.

02043. All users of systems used to store, process, or forward official information are to assent in writing to security monitoring of their activities before being given access to the system, and are required to annually reconfirm this assent in writing unless the logon process to the system itself displays an appropriate notification, as laid down at **Chapter 6**, which must be acknowledged before logging in successfully.

02044. The regulations relating to Personnel Security are laid down **at JSP440 Volume 2**, and these are amplified for CIS at **Annex F**.

02045. Joint Security Coordination Centre (JSyCC) The JSyCC is established to form a focal point for security Alert, Warning and Response (AWR) functions across defence. In respect of Information Security activities, JSyCC is responsible for:

a. Receiving and collating Security Intelligence relating to CIS, maintaining a central source of Vulnerability and Threat information, and promulgating Summaries, Alerts and Rectification Directives as necessary, in conjunction with similar organisations in UK Government, Law Enforcement, Industry and Allies;

b. Receiving and collating incident detection information, liaising as necessary with similar organisations in UK Government, Law Enforcement, Industry and Allies, and if required supervising any necessary response and post-incident analysis where such activity is inappropriate to be carried out at reporting unit level;

c. Supervision of all MOD Information Security Special Investigations (i.e. those relating to Compartmented material), particularly on behalf of the STRAP Management Committee (SMC) and other Compartment data owners;

d. Provision of MOD contribution to the National Infrastructure Security Coordination Centre's (NISCC) virtual organisation;

02046. Fuller details of the roles of JSyCC are given at **Chapter 11.** Outside core working hours, the MOD maintains an Information Security Duty Officer (ISyDO), which is a role fulfilled by members of DDefSy or JSyCC staff.

02047. Details of Incident Handling procedures, for both Detection and Response, within MOD are given in **Chapter 11**.

02048. Any significant or urgent Vulnerability and Threat alerts will be issued by JSyCC as either Vulnerability Warning Notices (VWNs) or Threat Warning Notices (TWNs), details of which are contained at **Annex G**. The requirements for acting upon VWN and TWN are laid down later in this Chapter, and units' requirements for subsequent Installation Vulnerability Validation (IVV) are detailed at **Chapter 12.**

02049. Details of the CIS Verification program, including both routine Inspections and Vulnerability Analysis, and the Enhanced Intruder Testing (EIT) program are given in **Chapter 12**.

Security Management Structures

02050. Security Working Group (SWG). An IT Security Working Group (SWG) must be established for all large, complex or operational CIS systems and projects. The SWG is to be formed from the outset for all CIS systems and projects, and is to be chaired by a senior member of the project/system staff, who will also provide resources, accommodation and administrative support for the SWG. The SWG is responsible for all aspects of security within the project or system and for supporting the accreditor and project sponsor. It reports to the project sponsor, accreditor and project board, and is to meet at frequent intervals, as determined by the project sponsor and accreditor,

throughout the whole lifespan of the project or system. Terms of Reference for a SWG are at **Annex H**.

02051. The SWG's function is to provide support to the project so that the accreditor is in a position to grant security authority to operate in due time and that any consequential changes to the project that affect security are recognised and suitable measures implemented. This implies responsibility throughout the whole life span of the project. In particular the SWG is to:

a. Assess the value of official information stored processed or forwarded handled by the project in all circumstances (such as "in barracks", in store, deployed on training, on operations and so on), by considering the outcome of loss of Confidentiality, Integrity or Availability, and allocate the appropriate protective marking;

b. Identify both general and particular vulnerabilities of assets making up the project, which could be exploited by a threat agency;

c. Identify both general and particular threat agencies that might exploit project vulnerabilities;

d. Assess appropriate countermeasures to reduce the consequent security risk to the project to an acceptable level in accordance with MOD policy and the needs of the project;

e. Arrange for the production, approval and promulgation of security documentation. Note that the documentation is to be agreed by the sponsor, the project office and the accreditor. The accreditor retains the responsibility for granting approval to operate.

02052. Installation Security Committee (ISC). An ISC is a variant upon the SWG, convened under the same Terms of Reference, but intended to cover IT Security issues for a number of different systems within a Site or Formation.

Accreditors

02053. The Accreditor is responsible for confirming that the specific implementation of any CIS has been appropriately secured in a duly diligent manner, taking account of national and departmental regulations, and as such does not present an unacceptable risk to national security.

02054. Within MOD, an Accreditor is a Competent Authority as recognised by either the DSO/and or the DSSO or one of the formally delegated PSyAs, tasked with performing CIS system Accreditation, and must be a member of MOD staff.

02055. It should be noted that the delegation of Accreditation Authority defined above refers solely to MOD owned material without specific Control or Release regulations. For systems storing or processing such material, **Annex D** to **Chapter 1**, which deals with the Protection of Compartmented Information, **must** be followed.

02056. The Accreditor's advice is to be sought from the outset for all CIS implementations, and where one a SWG is convened, the Accreditor is to be a full member of this group. For large, complex or operational CIS projects, the Accreditor should be consulted as to whether they wish a member of Tender Assessment Boards or to participate in higher-level Project Management Boards. Whenever security is on the agenda or may be discussed of other project meetings (e.g. discussions with industry and contractors), the Accreditor is to be consulted in advance. All decisions that may have an impact on any aspect of security and ITSEC or Common Criteria evaluation parameters should be agreed with the Accreditor.

02057. All security documentation, including amendments, is to be produced to the satisfaction of, and for approval by, the Accreditor before issue. Deviations to security policy and documentation (e.g. waivers and exceptions) may only be made with the prior permission of the Accreditor.

02058. The scope of a system is defined in terms of managerial responsibility. The Accreditor of a system will normally be similarly decided, but within each category of accreditation, the Accreditor(s) will fulfil one of a number of roles.

a. **Sole Accreditation**. A single Accreditor takes sole responsibility for all aspects of the system(s). Where a system crosses TLB or Trading Fund boundaries within MOD, the DSSO will normally assume this role, although the DSSO may choose to delegate this function to a PSyA where the majority of the system is within their remit, and only small elements cross into other PsyAs areas of responsibility;

b. **Joint Accreditation**. Where the system(s) to be accredited cross authority boundaries without MOD, such as into Allies or Other Government Departments (OGD), a number of Competent Authorities are required to endorse the system(s), co-ordinated through the fora of SWG and AP. The DSSO will normally assume the role of MOD Accreditor in such instances;

c. **Site or Formation Accreditation.** For large, replicated systems which cross TLB or Trading Fund boundaries within MOD, the endorsement of the security principles by the DSSO may optionally be carried out as a separate activity to the Site or Formation level implementation. In such cases, the appropriate PSyA will act as a Site or Formation Accreditor, ensuring that the installation specific concerns match both the general endorsed security principles and take due account of any specific local considerations.

02059. In cases where Compartmented Information is stored, processed or forwarded, in addition to Accreditation of the system, Compartment Approval must also be sought, in accordance with **Chapter 1 Annex D**. As with Accreditation, it is important that the Compartment Infosec Representative(s) (CIR) are approached as early as possible to ensure any additional requirements are identified. Should the CIR(s) not be known to project offices, then the DSSO should be consulted.

02060. Accreditation Panel. Where an CIS system does not fall solely within the boundaries of a single Accreditator's remit, connects to departments or organisations outside MOD, or holds information belonging to departments or organisations outside MOD, an Accreditation Panel (AP) will probably need to be established, with representatives for all Accreditors and from the Project Office. In most such cases, the DSSO will normally choose to staff the chairing of such panels.

02061. The AP will normally be an infrequent group, which would form only when specific Accreditation issues arise. They will be chaired by the "lead Accreditor", with secretariat functions provided by the affected project(s) or system(s). Routine Security issues should continue to be progressed through Security Working Groups (SWG). Membership would normally be restricted to the Accreditors and necessary CIS security agencies.

02062. There are a number of standing Accreditation Bodies in existence, for instance the Multinational Security Accreditation Board (MSAB) which deals with CCEB and NATO Accreditations, and projects should consult the DSSO when planning accreditation timescales, as there are benefits to defence in utilising such standing bodies rather than convening a multitude of separate APs with broadly similar representation.

Security Accreditation Principles

02063. An Accreditation is defined in HMG Infosec Standards as a formal statement by the Accreditor(s) confirming that the use of a system to store, process or forward Official Information under the conditions specified in the Security Policy Documentation (SPD) meets the security requirement and does not present an unacceptable risk. It is reviewed against the provision of adequate risk management procedures against all 8 facets of security as laid down at **Chapter 1**.

02064. Accreditation of a system or network is achieved by Security Staffs independently reviewing and agreeing the best fit of techniques and technologies to the Business needs. It therefore confirms, for both the Data Owner(s) and for the System Operating Authority (SOA), that Confidentiality provisions of the implementation do not present an unacceptable risk to the Information being processed, and that appropriate asset protection for Integrity and Availability is in place.

02065. The goal of the Accreditation process will be to gather evidence, to be presented to the Accreditor(s), that residual risks have be minimised to an acceptable level. For most non-technical facets of security, the evidence will be demonstration of compliance with MOD baseline security standards. For the 3 technical Infosec facets (Compusec, Comsec and Radsec), as well as compliance with baseline security standards, the organisation(s) responsible for the system's implementation should demonstrate that no significant exploitable vulnerabilities, or risks of failure of security functionality, exist.

02066. Additionally, Accreditation is required for the installation of additional equipment within an existing infrastructure, or for connection to existing systems or networks, to the connection will not adversely affect the security of the existing infrastructure.

02067. Accreditation is given on the basis of a both the Security Policy Documentation and physical instantiation(s). For sensitive or complex systems, the Accreditation will involve a detailed examination of system specific security requirements agreed between system management and security staff; and may require an assessment of the degree to which the system meets these requirements. For such systems, configuration control is of great importance. Further advice on Configuration Management is given at paragraph **02098** to this chapter.

02068. Although a Risk Management approach is taken, it must be realised that there are certain National Minimum Standards, including "baseline measures", with which MOD is obliged to comply.

02069. Where an accreditor exercises discretion to vary the requirement from that laid down in National or Departmental regulations, this will be done on the basis of a specific Risk Assessment for the system(s)affected. Requirements for dispensations **below** National Minimum Standards are laid down later in this chapter. In cases where an accreditor has to raise the requirements, the specific risks addressed **must be** documented in the SPD.

02070. To aid understanding of the way in which Accreditation is achieved and maintained, a generic schematic of how is given at **Annex I**.

Risk Acceptance

02071. The Accreditation process works in conjunction with the need for Operational Authorization, which is a subsequent management approval process whereby the System Operating Authority(s) (SOA) and Data Owner(s) accept any residual risks identified by the accreditation process. The Senior Responsible Officer is the individual who accepts the risk.

02072. An Accreditation Status, which will be issued in the form of a Certificate that should be held as part of the security register, can fall into one of 5 basic categories.

02073. Full Accreditation. The target for all permanently installed CIS should be to achieve Full Accreditation, which will be full compliance with all the SPD as endorsed by the Accreditor(s). In such circumstances, the Accreditation Certificate will be countersigned by the Accreditor and a representative of the System Operating Authority(s) (SOA) and Data Owner(s), and thereby grants Operational Authorization as well. An example of an Accreditation Certificate is given at **Annex I Appendix 1**.

02074. Interim Accreditation. Where a permanently installed CIS is does not fully meet the Target of Accreditation, but the shortfalls are as a result of a phased system development, a constrained **Interim** authorization (of limited duration and scope, as defined in the Certificate) can be issued instead, typically to permit Installation / Testing / Commissioning and "Initial Operating Capability" (IOC).

02075. In such circumstances, the Accreditation Certificate will be countersigned by the Accreditor and a representative of the System Operating Authority(s) (SOA) and Data Owner(s), and thereby grants Operational Authorization as well. It will be issued for a short period, normally of either 3 or 6 months, after which a review is required for renewal, and continual renewals are **not acceptable** as substitute for Full Accreditation. An example of an Accreditation Certificate is given at **Annex I Appendix 1**.

02076. Conditional Accreditation. For permanently installed CIS, which do not fully meet the Target of Accreditation whose shortfalls are of an unplanned nature (e.g. minor vulnerabilities found by Evaluation or from unscheduled minor changes), a constrained **Conditional** authorization (of limited duration and scope, as defined in the Certificate) can be issued. Conditional Accreditation can also be used in a planned manner for short duration installations such as Prototype/Demonstrator systems and quick notice deployments, where the full Accreditation cycle would be a nugatory effort. The need for Conditional Accreditation of short notice operations was formerly referred to as “Operational Exigency approvals”.

02077. In view of the increased risk being taken in such circumstances, the Accreditation Certificate as signed by the Accreditor will specifically itemised the shortfalls against the Target of Accreditation (for unplanned instances) or against national and departmental standards (for short duration installations). The countersignature in these cases must be made by a senior representative, of not less than 2* level, of the System Operating Authority(s) (SOA) and Data Owner(s) who in so doing accepts the risk, and thereby grants Operational Authorization.

02078. It is stressed that Conditional Accreditation must only be issued in respect of a CIS or Network **wholly within** the signatory’s jurisdiction. Conditional Accreditation will therefore not be permitted in a networked environment where such a decision could lead to a propagation of unacceptable risk(s) to the rest of the community, or where third party controlled or released information is stored or processed on the system(s).

02079. Conditional Accreditation can be issued for a maximum period up to 12 months, normally in 3 months renewable increments, and all Conditional Accreditations must be included in the Annual Report from the PSyA to the DSO. Continued renewal of Conditional Accreditations beyond a 12 month period is subject to review by the DSSO on behalf of the DSO. An example of an Accreditation Certificate is given at **Annex I Appendix 2**.

02080. Legacy Approval."Legacy" systems were retained systems which were installed before current security regulations were in force. Under Government wide requirements, all systems in that are service after 31 December 2000 must be Accredited. If there are therefore Legacy systems still non-compliant with either current Accreditation practices or National and/or Departmental standards, either the PSyA or DSSO must be contacted immediately the system(s) are identified to initiate Accreditation action. A summary of any Legacy Approvals found should be included in the PSyA annual report.

02081. Approval to Test (ATT) In addition to the Accreditation statuses listed above, Accreditors may also be requested to issue an "Approval to Test" (ATT) as a prelude to formalised Accreditation, which is intended to allow the installation and commissioning a system, but **does not normally permit the storage, processing or forwarding of Official Information**.

02082. It should be noted that Accreditation will become invalid if the particular use, configuration or environment of the system changes. It is therefore essential that before any proposed changes are implemented that they are discussed with the Accreditor, who will advise whether it is necessary to seek formal reaccreditation.

02083. The operation of non-Accredited CIS to store, process, or forward Official Information may be treated as a breach of security, and could result in confiscation or disconnection of the CIS by Security staffs.

Multinational Accreditation

02084. When operating in a multinational environment, it should be noted that NATO or Coalition documents may refer to Full Accreditation as "System Approval To Operate" (SATO), and/or Interim Accreditation as "Interim Approval To Operate" (IATO). Similarly, the term Designated Approving Authority (DAA) or System Approving Authority (SAA) will be encountered instead of Accreditor in NATO or Coalition documentation.

02085. Further details on multinational programmes are given at **Chapter 16**.

Evaluation and Certification

02086. Accreditation may need to be supported by Evaluation and Certification in accordance with Government Minimum Standards, or other MOD recognised formal

assurance activities. Details of these activities are given at **Chapter 6**, with the methodology for determining such requirements in MOD, an interpretation upon HMG Infosec Standard No. 1, contained at **Chapter 6 Annex B**.

Security Re-accreditation Procedure

02087. When it is proposed to effect a change, such as one of those listed below, to the configuration of a system, or to expand or extend an existing system, then re-accreditation procedures are to be implemented. The following gives guidance on when the Accreditor may require formal re-accreditation:

a. When an upgrade of hardware is to take place.

b. When an upgrade of the operating system is planned.

c. On the proposed extension or expansion of the system.

d. On a proposal of change of use of the system.

e. Where it is intended that a system authorised to process protectively marked data at one level intends to process data protected at another level.

f. When it is proposed to upgrade or change communication channels or equipment.

Dispensations

02088. Cases will arise where, on a Risk Management basis, a dispensation is required to permit operation of a system in cases where compliance with either National Minimum Standards, including "baseline measures", or system specific Accreditation requirements cannot be met. This may be for one of a number of reasons, the most common being:

a. Installation, testing and commissioning activities;

b. Limited operation (e.g. Initial Operational Capability);

c. Operational Exigencies;

02089. In most cases, the authority to operate in such a manner will accrue from a Conditional or Interim Accreditation, which identifies both the deficiencies, and the proposed way forward. However, in cases where the tolerance of such Accreditation is exceeded, then a specific dispensation should be sought, which may take one of 3 forms:

a. Waiver;

b. Exemption;

c. Dispensation.

02090. The PSyA will normally issue waivers, Exemptions and Dispensations, but for the following categories of system they can only be given with the explicit permission of the DSSO:

a. Systems used to store, process, or forward TOP SECRET material;

b. Systems used to store, process, or forward Compartmented ("Codeword" e.g. STRAP) material;

c. Systems used to store, process, or forward IDO owned material (e.g. NATO);

d. Systems used to store, process, or forward UK EYES material;

e. Systems defined as being Criticality Level 1 (CL1);

f. Systems crossing TLB boundaries;

g. Systems connecting outside of MOD boundaries (e.g. to Allies or OGD)

h. Generic waivers, exemptions or dispensations affecting multiple systems.

02091. Wavers, Exemptions and Dispensations are issued by PSyAs on a case-by-case basis, and cannot be construed to constitute any form of precedent, as such a course would be deemed to be an application for a generic approval, which will automatically require reference to the DSSO.

02092. Waiver. A waiver is a risk management tool that allows rules to be waived, in extraordinary circumstances, for periods up to one year, when it is judged that a temporary deviation will not result in any vulnerability being exploited. Accordingly, a waiver gives approval for the temporary deviation from the mandatory standards in circumstances where:

a. Essentially the same level of security is afforded and compensatory measures are not required; or,

b. A vulnerability has been created and acceptable compensatory measures have been applied; or,

c. A vulnerability exists and, despite the application of all feasible counter measures, remains extant.

02093. If renewal of a waiver is required, a revised case, justifying its continuance is to be submitted through the PSyA to the DSSO as a request for an exemption.

02094. Exemption. An exemption is similar to a waiver but applies where there is a need for long-term dispensation. The likelihood of a vulnerability being exploited will increase with duration, frequency and predictability. Accordingly, an exemption will only give approval for the long-term deviation from the mandatory standards in circumstances where:

a. Essentially the same level of security is afforded and compensatory measures are not required; or,

b. All feasible compensatory measures have been taken and nothing more can be done.

02095. Exemptions are to be reviewed every 5 years. A list of exemptions is to be included in the PSyAs Annual Reports to D Def Sy.

02096. Full Dispensation: no time limit, but Security Policy Documentation must reflect the details of the Dispensation, including the details of the issuing Competent Authority.

02097. In the case of non-compliance with system specific Accreditation requirements, Waivers may be issued by any Competent Authority with specific delegation of such powers through the Security chain of command, and both Exemptions and Full Dispensations by PSyAs. In all cases of non-compliance with National Minimum Standards, including "baseline measures", the DSSO should be consulted via the Security chain of command before issuing a Dispensation.

Configuration Management

02098. Configuration. Configuration is the general term given to an IT system to identify and describe its hardware, software and firmware. The configuration also includes the physical layout, connection of the component parts and software version information.

02099. Configuration Management. Configuration management consists of identifying, controlling, accounting for, disseminating and auditing all operation, maintenance and enhancement (including software) of a system. Configuration management is to be implemented as early as the system design stage and will remain in force until the system reaches the end of its useful life.

02100. This will not only encompass the security features provided by hardware, software and firmware security measures where these exist but also the operating system and application packages.

Configuration Management Responsibilities

02101. The System Manager/Project Officer or nominated deputy is to be responsible for the control and organization of the system of recording configuration updates. This includes all software changes (new issues and fixes/patches), upgrades of hardware and changes to the system communication etc, including plans to expand or extend the system.

Configuration Plan

02102. As a guide this should cover:

a. The controls (technical, physical and procedural), applicable to the protection, from unauthorized modification or destruction, of the hardware and master copy or copies of all material used to generate the system, including utilities and software packages.

b. System hardware, firmware and software configuration modification request procedures.

c. Specific modification request procedures for the hardware configuration, or system related environment, where there is a need to comply with a TEMPEST standard; and specific post modification testing and monitoring to ensure that standards are being met and complied with.

Procedures for Expanding the System

02103. Where it is planned to expand or extend a system, the following controls are to be implemented:

g. The ITSO or nominated deputy is to seek initial security authority for the proposed change.

h. Where the change will impact on TEMPEST controls in force, advice is to be sought from the relevant IDA for the existing system.

Oversight

02104. The accreditation of CIS within MOD is largely delegated by the DSO to the DSSO and PSyAs, who may have further sub-delegated accreditation powers.

02105. The DSO, however, retains the right, irrespective of any delegation(s), to review the Accreditation of any CIS installation within the Defence ambit, including industry and agencies. This will in certain cases override the need for local sponsorship for a visit.

02106. The DSSO provides an independent security audit capability to enable the DSO to certify that security policy is being implemented adequately and cost-effectively across the whole of MOD and its Trading Funds

Accreditation Review and Appeals

02107. Accreditation is exercised by the delegated Accreditors on a Risk Management basis, and inherently will involve the exercise of discretion in reaching a decision as to whether or not to Accredit a CIS, and what conditions, if any, are required in granting an Accreditation.

02108. To guard against any perception of abuse of discretion, a review and appeals procedure is provided:

a. For Appeals by System Operating Authorities (SOA) or Project Management Authorities (PMA) who either feel that a decision to not accredit a CIS within their ambit has been incorrectly taken, or where there is a perception of unequal treatment being afforded to other CIS. This mechanism is also to be used by PMA involved in Procurement where contractor(s) allege unfair treatment by Accreditors, and is in such cases must be agreed to be binding arbitration;

b. For Review where another Competent Authority (e.g. CESG or OGD/Allied Accreditor) believe that a decision to accredit or not accredit a CIS has been incorrectly taken, or where there is a perception of unequal treatment being afforded between CIS.

02109. In such cases, the PSyA(s) for the TLB(s) involved should initially be contacted for a review of the decision. In cases where it is the decision of the PSyA(s) themselves that are called in to question, or where an impasse has been reached where more than one Security Authority is involved, the DSSO will act as the final arbiter of such Appeals.

Dispensation Review

02110. In cases where compliance with either National Minimum Standards, including "baseline measures", or system specific Accreditation requirements cannot be met, the Accreditor may, on Risk Management basis, need to grant or seek a dispensation.

02111. Such dispensations are subject to periodic review.

02112. In the case of Waiver, when renewal after the initial 12 month maximum period is required. In these instances a revised case, justifying its continuance is to be submitted through the Security Authority to DSSO as a request for an exemption.

02113. In the case of Exemptions, the case for their continuance is to be reviewed every 5 years. A list of Exemptions is to be included in the PSyAs Annual Reports to D Def Sy.

02114. In the case of Full Dispensations issued by PSyAs, a list of Exemptions is to be included in the Annual Reports to D Def Sy.

02115. In all cases of non-compliance with National Minimum Standards, including "baseline measures", DSSO should be consulted via the Security chain of command before issuing a Dispensation.

Security Compliance

02116. The achievement of Accreditation for a system declares that an Accreditor, as a Competent Authority has reviewed and accepted the Risks and their Management for the system(s) as installed. The validity of this situation can only endure as long as the Risks do not change, and the configuration is unchanged.

02117. To maintain effective security for the lifetime of a system, in addition to the measures inherent in Project Management structures such as Security Working Groups (SWG) and Configuration Management (CM) Boards, additional procedures are required that ensure ongoing compliance with security requirements until the system is finally withdrawn.

02118. Within the MOD environment, all activities are implicitly liable to review to ensure that the relevant procedures and regulations are being complied with. It is therefore inherent that any system used to store, process or forward Official Information may be subject to technical or procedural compliance review by appropriate MOD Security Authority staffs, or other Competent Bodies agreeable to MOD Security Authorities, with or without the knowledge of its users.

02119. In order to achieve continuance of compliance, 3 specific classes of security compliance activities are identified, which are defined as being:

a. Oversight;

b. Compliance;

c. Incident Response.

02120. The subjects of Compliance and Incident Response are complex topics in their own right, and have Chapters of this Volume dedicated to them, with Incident Handling forming **Chapter 11** and Compliance forming **Chapter 12**.

Responding to Warning Notices

02121. The System Operating Authority (SOA) is responsible for ensuring that appropriate action, to avoid exploitation by any potential attacker, is taken on receipt of any Threat or Vulnerability alerts issued by JSyCC, as discussed in this Chapter.

02122. Threat. JSyCC promulgates both Threat Warning Notices (TWN), which relate to specific Information Security Threats, and Threats Change Notices (TCN), which advise of modifications to the overall "Cannel" Levels.

02123. The action required upon the receipt of a TWN will be dependent on the specific content of the alert.

02124. The action required upon the receipt of a TCN is a combination of the Cannel Level and the Criticality Level of the system, as laid down in the following table:

Cannel Level	**Criticality Level**			
	CL4	**CL3**	**CL2**	**CL1**
RED	As laid down in Rectification Directive			
AMBER	Weekly	Daily	Daily	Immediate
BLACK	Weekly	Weekly	Daily	Daily
WHITE	Monthly	Weekly	Weekly	Daily

02125. Vulnerability (including Malicious Software). JSyCC issue both Alerts - Vulnerability Warning Notices (VWN) or Vulnerability Rectification Directives (VRD), each of which will have a generic measure of severity associated with it. System Operating Authority (SOA) are required to initiate remediation for the Vulnerabilities within the following timescales:

Severity Class	**Criticality Level**			
	CL4	**CL3**	**CL2**	**CL1**
VERY HIGH	As laid down in Rectification Directive			
HIGH	Weekly	Daily	Daily	Immediate
MEDIUM	Weekly	Weekly	Daily	Daily
LOW	Monthly	Weekly	Weekly	Daily
VERY LOW	Monthly	Monthly	Weekly	Weekly

02126. Specific procedures for acting on VWN received in respect of Malicious Software are laid down at **Chapter 7**.

02127. Where Vulnerability Rectification Directives (VRD) have been issued, PSyAs are responsible for collating progress against these VRD within their area of responsibility (AOR), and providing progress summaries to JSyCC.

02128. Compliance with other VWNs is achieved through the practice of Installation Vulnerability Validation (IVV), as laid down at **Chapter 12**.Further information on Vulnerability and Threat Warning Notices is given in **Annex G** to this Chapter.

Incident Reporting

02129. Any hardware or software security weakness, malicious software attack and other security related incidents or weaknesses must be reported. The MOD is a contributing Department to the Government wide Unified Incident and Reporting Scheme (UNIRAS). The rules for incident reporting are covered in **Chapter 11**.

Security Inspections

02130. The DSO retains the right, irrespective of any delegation(s), to inspect without warning any IT installation within the Defence ambit, including industry and agencies. This will in certain cases override the need for local sponsorship for a visit.

Awareness, Education and Training

02131. It is essential for the maintenance of an effective information security program across Defence that all interested parties, including Data Owners, System Operating Authorities (SOA), and end users, are aware of the issues, and that practitioners are provided with appropriate Education and Training.

02132. Awareness. The main vehicle for the promulgation of general information security information across all personnel in Defence is this manual, augmented as required by Defence Council Instructions (DCI). This is supplemented by additional background information provided on various Intranet web severs, and included as part of the Security section of the DCSA Catalogue for those users not having access to the main intranets.

02133. Additionally, the Joint Security Coordination Centre (JSyCC) publishes Threat and Vulnerability information to Security and CIS staffs, details of which are provided in this Chapter. Furthermore, current news items in the Information Security field are available on request from the JSyCC, in either direct feed or digest form, to those having access to either Intranet or Internet mail.

02134. ITSOs are recommended to run local Information Security Awareness initiatives to ensure all staff within their area maintain some exposure to the issues. At the simplest this could be a paper circulation of DCIs and local Security Operating Procedures (SyOPs), to ensure these are seen, and signed for, by all staff. Should ITSOs wish to run dedicated Awareness events, the PSyA should be consulted for assistance in their organisation.

02135. Should course directors or event organisers wish to include one or more Information Security sessions within courses or events that they intend to run, D Def Sy should be contacted in the first instance for advice.

02136. Education and Training. A number of different avenues for formal Information Security education and training are open to MOD staff with either CIS or Security responsibilities, the main ones being:

a. ITSO training on the Fundamentals of Information Technology Security course at DISC Chicksands;

b. Computer Installation Manager's course and Computer Security course at CSTF RAF Halton;

c. A variety of specialist courses run at the Civil Service College, most with MOD visiting lecturer support;

d. Installation Designer training at DCSA Swindon;

e. IT Health Check training at DERA Malvern;

f. Courses run by the Communications-Electronic Security Group (CESG);

g. Courses run by the Security Service;

h. Commercially provided courses on niche technical subjects.

02137. These courses are designed both to provide pre-employment training for designated posts, and to provide means to infuse additional training as required for existing practitioners.

02138. An annual DCI GEN is published by D Def Sy summarising all the MOD and Government provided courses. Before contracting for commercially provided courses, units are advised to consult either their PSyA or D Def Sy.

02139. It is essential that having completed any relevant formal training, practitioners are afforded with the opportunity for Continuing Professional Development (CPD). This need should be reflected in annual training plans for such posts, and, where applicable, as Investor in People (IIP) objectives.

02140. At present, there is no single organisation, which MOD can recognise as providing the prime professional body for Information Security practitioners, although this situation is being actively monitored by D Def Sy, and as such there is no single path for CPD.

02141. To aid the need for CPD, PSyAs may run seminars or roadshows for staff within their TLBs, details of which can be obtain direct from these authorities.

02142. The Defence Infosec Product Coordination Group (DIPCOG) runs a series of Open Days for CIS and Security staffs where security product vendors are invited to showcase new technologies, which will include briefing sessions covering MOD and Governmental policy and organisational updates by D Def Sy and EC-CCII-IOCM.

02143. Additionally, a number of commercial Conferences and Exhibitions are available annually both in the UK and overseas covering Information Security topics, some of which will include presentations and/or exhibitions from MOD and/or Government sources. A list of these conferences is maintained the DIPCOG, and is available from PSyAs, on some Intranet web servers, and is included as part of the Security section of the DCSA Catalogue for those users not having access to the main intranets. It should be noted overseas conferences may sometimes be found to be better value than those in UK, either due to the wider number of streams available and/or due to the total cost to unit budgets often being less than what are normally expensive UK conferences.

02144. Some existing recognised professional bodies (e.g. the British Computer Society) do cover Information Security specialisms, and, where appropriate to their role, practitioners are encouraged to seek membership of such organisations, which may offer their own CPD routes, although these will not completely meet MOD CPD requirements.

02145. Until MOD is able to formally recognise CPD options afforded by external professional bodies therefore, the following framework should be taken as guidance as to the level of effort likely be required for maintenance of Information Security currency amongst MOD practitioners:

Role	CPD Suggested
Part time IT Security Officers (ITSO)	• At least 1 day every other year • Biennial MOD and Governmental policy and organisational updates • Biennial attendance at appropriate UK exhibition
Full time IT Security Officers (ITSO)	• At least one day per annum • Annual MOD and Governmental policy and organisational updates • Annual attendance at appropriate UK exhibition • Consider attendance at appropriate UK conference

System / Network Security Officer	• At least one day per annum • Annual MOD and Governmental policy and organisational updates • Annual attendance at appropriate UK exhibition • Appropriate specialist training to meet evolution of technologies involved
Installation Design staff	• At least 1 day every other year • Biennial MOD and Governmental policy and organisational updates • Biennial attendance at appropriate UK exhibition
Security Assurance Coordinators (SAC) - and -Delegated Accreditors	• At least 3 days per annum • Annual MOD and Governmental policy and organisational updates • Annual attendance at appropriate conference(s) • Appropriate specialist training to meet evolution of technologies involved
PSyA or delegated Accreditors - and -Policy staffs	• At least 5 days per annum • Annual MOD and Governmental policy and organisational updates • Annual attendance at appropriate conference(s) • Appropriate specialist training to meet evolution of technologies involved

This page is intentionally left blank.

ANNEX A TO

CHAPTER 2

INFORMATION TECHNOLOGY SECURITY OFFICER (ITSO)

Generic Responsibilities

1. The post of ITSO has been established to address the problems encountered with unit-level administration of security for IT systems.

2. The Commanding Officer/Head of Establishment (CO/Hd of E) is responsible for the appointment of an ITSO. The appointment is subject to endorsement by the TLB Principal Security Adviser (PSyA) if appropriate.

3. The ITSO is responsible to the CO/Hd of E for all IT systems security within the unit/establishment, although for larger systems (eg CHOTS) may only be acting in a liaison capacity with a dedicated System or Network Security Officer.

4. The post is a security rather than an IT function, and care must be taken to avoid conflict of interests if appointing IT staff into such posts to ensure segregation of responsibility.

5. The ITSO and ESyO will need to interact to ensure overall security is maintained.

6. The unit/establishment wide tasks of the ITSO are:

a. Providing security advice to the installation staff and system users and, where appropriate organising Installation Security Committees (ISC).

b. Monitoring the implementation of hardware and software modifications and enhancements to ensure that security is not breached and, as appropriate, ensuring that security implications are considered at Change Control Committees (CCC)/Configuration Management Boards (CMB).

c. Liaising with contractors to ensure that maintenance is carried out without endangering security.

d. Reporting to the PSyA security staff or DSO where appropriate, any security loopholes, infringements and vulnerabilities which may come to light.

e. Liaising with the PSyA security staff or DSO where necessary.

f. Preparing security reports and conducting security surveys required by the CO/Hd of E.

7. The tasks that the ITSO must either carry out, or ensure are performed in respect of individual systems by Installation Security Officers (ISO) are:

a. Maintaining a security log which, in conjunction with the system log (which may be maintained by the SM or NW Manager), should record sufficient details about the normal activities of the system to enable a history of events to be reconstructed. The security log should monitor and record activities (against times and dates) which could jeopardise the security of the system including:

(1) Abnormal termination of a job or abnormal system shutdown

(2) Failure of security mechanisms

(3) Unauthorized attempts to gain access to classified data or use of system facilities in an unauthorized way.

(4) Suspected attacks from malicious software.

b. Ensuring that the security maintenance and system logs are examined and countersigned by the ESyO at intervals decided by the DSO.

c. Ensuring that all personnel having access to the installation are appropriately security cleared or supervised and are aware of the local security regulations, maintaining a record of all persons authorized to use any part of the systems and the extent of their authorizations, and arranging for suitable security education for all installation staff and system users.

d. Issuing of passwords or other access control devices (if both are in use, the ITSO should be responsible for issuing one or the other but not both).

e. Ensuring that visual checks are made on equipment for signs of tampering and that the inspections are recorded in the security log.

f. Ensuring the proper custody of classified magnetic media and other installation IT documents. Sampling checks should be made and recorded at irregular intervals (but at least monthly) on the presence of these media and on the accuracy of their markings.

g. Before the release from installations of media which have undergone the approved declassification procedure, ensuring that they do not in fact bear

protectively marked data and that external signs which might permit deductions to be drawn about previous usage are removed.

8. To fulfil this role, the following selection criteria of competencies should be applied:

a. Holding an appropriate security clearance and protective briefing(s)sufficient to access all areas within the unit/establishment in order to deal with any incidents that may arise on systems therein.

b. Security training: The Fundamentals of Information Technology Security Course at the Defence Intelligence and Security School (DISS) or equivalent. If necessary the courses below should also be attended.

(1) An Introduction to Infosec (if no previous experience)

(2) Infosec for Practitioners

(3) TEMPEST Basics and Familiarization

c. IT Training: Fundamentals of Computing (if no previous experience)

d. The details of these and other courses are published annually in a DCI GEN. There may be appropriate Single Service Courses available as an alternative.

This page intentionally left blank.

ANNEX B

TO CHAPTER 2

SECURITY RESPONSIBILITIES OF A SYSTEM OPERATING AUTHORITY

1. The responsibilities of a System Operating Authority (SOA) include:

a. Defining the boundaries of the system and designating secure areas.

b. Determining how the regulations in this Manual are to be implemented in the system (consulting the SWG as appropriate).

c. Producing and maintaining a Security Policy Documentation (SPD), agreed with the security authorities, stating the security requirements for the system.

d. Determining the Security Processing Mode and seeking approval for it from the appropriate authority, via the Security Chain of Command.

e. When directed, arranging for independent testing of the system, including any remote site, and inspection of, its documentation.

f. In consultation with the security staff, determining the appropriate security measures required, by means of a risk assessment, and preparing the system Security Operating Procedures (SyOPs) for approval by the security authority.

g. Ensuring that no protectively marked work is undertaken unless the appropriate approved SyOPs, including vetting of staff to the requisite level, are in force (i.e. the system meets its accreditation standards).

h. Ensuring that material originated for management or maintenance purposes is correctly protectively marked.

i. Issuing security guidance and instructions to the system users, including appropriate training.

j. Ensuring the secure use of data links and remote terminals. He or she must not allow connection of a terminal until all security requirements have been met, and must keep the security arrangements of each remote terminal under constant review in conjunction with the Commanding Officer or Head of Establishment of the unit in which the system is situated.

k. Arranging the necessary supervision and control of all maintenance and repairs, especially when carried out by civilian contractors.

l. Ensuring that validation checks are carried out when changes are made to the system controlling/operating software.

m. Appointing an SSO and, where relevant, a NSO, and ensuring the security of remote terminals.

n. Establishing, where appropriate, a SWG.

o. The auditing of the system status accounting procedures.

ANNEX C TO

CHAPTER 2

SECURITY RESPONSIBILITIES OF A SYSTEM SECURITY OFFICER (SSO)

1. The responsibilities of a System Security Officer include:

a. Maintaining SyOPs for the system, and circulating SyOPs to staff on a regular basis.

b. Providing system security advice to the system's management, system staff, and system users.

c. Briefing staff on system security responsibilities.

d. Ensuring that all personnel having access to the system are appropriately security cleared and/or supervised, and are aware of the local security regulations.

e. Maintaining a record of all persons authorized to use any part of the system, and the extent of their authorization.

f. Controlling and issuing passwords or other access control devices where relevant.

g. Monitoring and implementing hardware, firmware, and software modifications and enhancements to the system to ensure that security is not breached.

h. Ensuring that records of hardware, firmware, and software changes and defects are kept and regularly examined for unusual trends.

i. Liaison with contractors to ensure that maintenance is carried out without endangering security.

j. Ensuring the proper custody of magnetic media and other system documents.

k. Carrying out sampling checks and maintaining records of checks, at agreed intervals, on the presence of protectively marked magnetic media and other system documents.

l. Ensuring that before their release from the system, checks are made on documents which have undergone an approved declassification procedure to show that they do not, in fact, contain protectively marked data and that the external signs which might permit deductions to be drawn about previous usage are removed.

m. Maintaining and examining system security logs which should record sufficient details about the normal activities of the system to enable a history of events to be reconstructed. The security log should include monitoring and recording of activities (against date, time, and user) which jeopardize the security of the system, including:

(1) Start-up and shut-down of the system, including abnormal termination.

(2) Failure of system security mechanisms.

(3) Unauthorized attempts to gain access to protectively marked data or make use of system facilities in an unauthorized way.

(4) Suspected attacks from malicious software.

n. Monitoring the back-up and recovery of system security relevant information.

o. Monitoring the configuration management aspects of changes to security-related hardware, firmware, or software and associated documentation.

p. Reporting any system security loopholes, infringements, and vulnerabilities which may come to light, to the System Manager and the appropriate accreditor(s).

q. In conjunction with the accreditor(s), initiating any security investigation into possible security breaches involving protectively marked information.

r. Liaison with the appropriate accreditor(s) on all aspects of system security.

ANNEX D TO

CHAPTER 2

TERMS OF REFERENCE FOR THE SECURITY ASSURANCE COORDINATOR (SAC)

1. The Security Assurance Coordinator (SAC) is a member of the PRINCE Project Assurance Team. The SAC will receive direction from the Accreditor, the Project Board, the Project Manager and Stage Manager. He will work in co-operation with the Configuration Librarian, the Business Assurance Co-ordinator, the User Assurance Coordinator and the Technical Assurance Co-ordinator.

2. The SAC must have a sound understanding of how electronic security measures are designed and implemented in secure systems. He must have a good working knowledge of configuration management practices for secure systems and he must be aware of the importance of procedures which can provide traceability in software.

3. The SAC should have attended the Implementing Infosec course or an equivalent and should have received formal training in communications and network security. It is recommended that contractors employed as SACs should either be an accredited BS7799 auditor or on the CESG Listed Advisor Scheme.

4. The SAC will report on security matters to the Accreditor. He will present unresolved difficulties to the Security Working Group (SWG), co-ordinate security functions among the SWG and carry out the decisions of the SWG.

5. The SAC advises, monitors and reports on security matters relating to the project and may on occasions chair the SWG on behalf of the Project Manager. His main tasks are to:

a. provide advice on security policy and technical solutions;

b. ensure that security policy is being correctly applied;

c. monitor security considerations that are being incorporated and report on them to the Security Working Group;

d. highlight and report unresolved security difficulties to the Security Working Group;

e. organise the project Security Working Group meetings;

f. inform the Project Board, through the Project Manager, of the Security Working Group decisions;

g. ensure that the configuration management procedures meet the criteria for the required level of assurance;

h. channel advice from the National Security Authorities advisers and TLB Principal Security Advisers (PSyA) to the SWG;

i. ensure that the deliverables are made available at appropriate times;

j. ensure that the appropriate authorities are informed of the non-electronic security measures that the system will rely upon when it is in service;

k. establish the terms of reference for the SWG;

ANNEX E TO

CHAPTER 2

INSTALLATION DESIGN AUTHORITY (IDA) AND COORDINATING INSTALLATION DESIGN AUTHORITY (CIDA)

Introduction and Scope

1. This Annex gives details of the procedures required to ensure the basic technical security of IT equipment used within the MOD and applies in **all** instances, even if the equipment does not store or process protectively marked information. It should be noted that all IT equipment requires security approval and the relevant security authority should be consulted in the first instance, before procurement begins.

Principles

2. In order to ensure the Confidentiality, Integrity and Availability of all IT equipment within the MOD, and to comply with both National and MOD regulations, it is essential that the relevant security authority and IDA and/or CIDA are notified **in advance** of **all** new requirements and/or when changes to the type(s), location(s), classifications or number(s) of equipments installed are proposed. The CIDA will vet all designs and proposals of new systems and incorporate them into existing drawings and plans (See **Appendix 1**).

3. The primary concern is that systems processing protectively marked information are installed and operated in such a way that they do not compromise their own security, or that of other systems in the vicinity. It is also important that Unclassified systems are reviewed by the appropriate security authority, both to ensure that the equipment and its installation does not affect or assist in the escape of emanations from classified systems (TEMPEST), and to minimise the risks to the confidentiality, integrity and availability of systems and data (eg from "hacker" and virus attacks).

Responsibilities

4. It is the responsibility of Branch/Unit Security Officers to ensure that the relevant National and MOD regulations are applied within branches, although for larger systems the Project Office may assume responsibility for all branches using the system.

5. The security staff is responsible for ensuring that protectively marked information is protected and that IT systems dealing with such data are accredited. There may often be a local Establishment level security officer through whom the request should be made.

6. The IDA and/or CIDA are responsible for ensuring that all equipment is installed and operated in such a way that it does not compromise the equipment's safety or security, or that of other systems in the vicinity. This will include security measures and technical countermeasures being implemented as required and the maintenance of good engineering practices to comply with national regulations. In some areas there is a requirement that all such requests are passed to the Establishment/Building Services manager.

7. The central contact/advisory points for both security and installations concerns are given in the table below. If there is any doubt as to whom the IDA/CIDA for an area is the relevant TLB Principal Security Adviser (PSyA) should be consulted.

CO-ORDINATING INSTALLATION DESIGN AUTHORITIES

TLB AREA	**BRANCH**	**ADDRESS**	**TELEPHONE**
MOD HQ, Centre and DPA, DLO:	DCSA CIM1	Minerva House Swindon	5353 MIN Fax 5359 MIN
Royal Navy:	DCIS(FS)	Fort Southwick Fareham	428 FW Fax 5444 FW
Royal Air Force:	DS6 RAFSEE	RAF Henlow Beds	7886 HEN Fax 7687 HEN
Army:	CIDA, CPD, Army CIS Engineering Group	 Blandford Camp Blandford Forum	 5277 BLN Fax 5461 BLN
DSTL:	IT Security Adviser	DSTL Room D43 East Court Portsdown	 01684 894531 Fax 01684 896070
Meteorological Office:	CIDA Manager	Easthampstead Beaufort Park Wokingham	 01344 855616 Fax 01344 855878

Factors

8. Appendix 1 lists the main items of information that will be required by the security authority and (C)IDA and this should be obtained before seeking any clearance for either security or installation design approval.

Summary

9. All IT systems used to process, store or forward information, as defined in paragraph 2 above, require security and installation approval. This approval may include additional requirements, to comply with British TEMPEST Regulations which can increase the overall project costs. Early contact with the relevant authorities is essential to ensure that adequate funding is available.

This page intentionally left blank.

APPENDIX 1 TO

ANNEX E TO

CHAPTER 2

INFORMATION TO BE SUPPLIED WHEN SEEKING APPROVAL FOR CIS

1. Security and (Co-ordinating) Installation Design Authority.

a. Ship/Submarine/location and site/building with position relative to the nearest non-MOD controlled area.

b. Is the building solely MOD use, OGD or shared.

c. Location of the room(s) within the site, with a general floor plan showing any party features.

d. Details of the level of protective marking in use and proposed, including CAVEATS or CODEWORDS.

e. Details of the equipment proposed to be used, both for the computer systems and any associated communications equipments.

f. Existing approvals and Security Operating Procedures (SyOPs) for equipment in the branch and or location.

g. Details of the physical protection available (doors,windows,cabinets).

h. Details of any nearby RF transmission equipment.

i. Details of any electromagnetic screening installed.

j. Details of any existing TEMPEST counter-measures (RF filters on mains and signal cables, extended RED areas etc).

k. Details of CIDA/IDA responsibilities for the department under scrutiny and POCs within the department who are authorised to sign release forms for the purchase of new IT equipment.

2. **(Co-ordinating) Installation Design Authority only.**

a. Detailed plan showing positions of all electronic and telephone equipment (eg computers, audio visual equipment, FAX, printers, answerphones, switches and microwave ovens) installed or planned to be installed, including routing of associated cables.

b. For shared accommodation: whether the MOD have either their own switchboard or, if not, whether telephones are filtered at the point of entry to MOD areas.

c. Details of mains outlets and sockets.

d. Details, if possible, whether the mains supply is provided by a dedicated, on site, transformer. If in shared property, whether the MOD have either their own phase(s) and whether the supply is filtered at the point of entry to MOD areas.

e. Details of any electromagnetic equipment installed in adjacent spaces (in 3 dimensions).

f. Office furniture.

ANNEX F TO

CHAPTER 2

PERSONNEL SECURITY FOR CIS

Threats

1. Disaffected or dishonest staff may threaten valuable information and assets in various ways, either on their own behalf or as agents of others. Threats to CIS system security can arise from any individual who has the necessary level of expertise and knowledge of the system and requisite access to the system. It is also possible that someone with the necessary expertise could school an inexpert accomplice to carry out actions by proxy. It follows that staff with legitimate entry to CIS facilities may have unique opportunities for the unauthorized and surreptitious acquisition of information, for tampering with the data or for permitting its extraction by unauthorized persons.

Counter Measures

2. **Vetting.**

a. All authorized users are to have security approval appropriate to the highest level of data processed/stored by the CIS system or commensurate with the Mode of Secure Operation.

b. Security approval may be required for personnel who do not have direct access to the system but whose duties bring them regularly into offices where the system is located.

c. SyOPs are to detail the appropriate level of clearance for all personnel who have direct access to the system and similarly those whose duties bring them regularly into offices where CIS systems are located.

3. **Access.**

a. The Security Policy Documentation will detail the specific requirement for access, in particular where the two person rule applies. System specific regulations are to be included.

b. The ITSO is responsible for ensuring that no person has direct or indirect access to the CIS system without proof of security approval. SyOPs are to detail the action to be taken when ancillary staff such as cleaners and workmen are present in offices where the system is located.

c. SyOPs are to detail circumstances where the 'Two Person Rule' should be in operation, and who is to be involved. In addition to the standing requirements covering the processing of protectively marked information, this will also be required when technical staff such as CIS manufacturers, system designers, engineers and other technical staff who by virtue of their knowledge of, and potential access to, the system hardware and software have an opportunity for the surreptitious compromise of the system.

d. Should a person with authorized access to a system come to adverse security notice, then SyOPs are to detail the procedures to be carried out, including denial of access, until the situation is resolved.

4. **Supervision.**

a. Supervisors of staff with authorized access to sensitive CIS systems are to pay particular attention to any signs of unreliability. Where it appears that staff may become disaffected due perhaps to disciplinary or redundancy action, it may be necessary to deny staff their usual access to a system.

b. Uncleared staff requiring access to areas where protectively marked information is, or may be exposed, are to be supervised at all times.

c. It should not be assumed that a person's capability for attacking a system is limited by their function, knowledge or expertise; their activities could be directed by others.

5. **Security Awareness.**

a. All staff with access to CIS systems are to be instructed on the security regulations and procedures they are expected to comply with or are responsible for. They are periodically to be provided with a set of SyOPs and are to sign that they have read and understood them.

b. No member of staff is to be allowed access to an CIS system until they have received a security brief.

ANNEX G TO

CHAPTER 2

VULNERABILITY AND THREAT ALERTS

1. Responsibility for the dissemination of security intelligence Alert and Warning (A&W) information relating to CIS across MOD lies with the Joint Security Coordination Centre (JSyCC). The following table summarises the types of information A&W that may be expected :

A&W Aspect	Priority	Notification Type	Primary Dissemination
Threat	Urgent	Threat Change Notice (TCN)	Signal message
	Routine	Threat Warning Notices (TWN)	Email
Vulnerability	Urgent	Vulnerability Rectification Directive (VRD)	Signal message
	Routine	Vulnerability Warning Notices (VWN)	Email
Threat and Vulnerability	Routine	Request For Information (RFI)	Email

2. It should be noted that these notices refer solely to CIS Vulnerabilities and Information Security Threats. Non-Information Security Threats, such as the Bikini, Tahiti and Tesseral systems, are the responsibility of the DDefSy Threat Desk and will generally be promulgated via the Security Chain of Command.

3. All JSyCC A&W material bears a serial number in the format :

JSYCC/A&W/xxx/yyyymmdd-nn[-a]

where : xxx Notification Type
yyyy Year
mm Month
dd Date
nn Serial Number
[-a] Edition Number

4. Where updates are issued, these will be issued as supplementary editions to the original version.

5. A listing of all extant JSyCC A&W material is provided on a Web Page available within the DGS&S area of MODWeb, and on other intranets taking feeds from MODWeb.

Vulnerability Information

6. Vulnerabilities are graded according to their severity, in line with the following table:

Vulnerability Class	Threat	Impact
A (Extreme)	Very High	High
B (Significant)	High	
C (Major)	Significant	Medium
D	Moderate	
E (Minor)	Low	Low
F	Negligible	

7. Only Vulnerabilities grade at Class D or greater will normally be promulgated by VWN, with VRDs being reserved for Class A vulnerabilities, but the JSyCC maintains a database of all current known vulnerabilities which can be searched on request.

8. The majority of VWN and VRDs will be the MOD instantiation of the information received from the Unified Incident Reporting and Alerting Scheme (UNIRAS), operated by the UK National Infrastructure Security Co-ordination Centre. UNIRAS Briefings will normally be issues as VWN, and UNIRAS Alerts as VRD. As some MOD units may also receive copies of UNIRAS material by other route, a Web Page is available within the DGS&S area of MODWeb, and other intranets taking feeds from MODWeb, showing a mapping between the JSyCC A&W reference and the UNIRAS reference.

9. In addition to the UNIRAS information, JSyCC may from time to time issue WN or VRD from other sources, such as that obtained from Dstl, from Allies through for a such as the Military Federation of Incident Response and Security Teams (MILFIRST), in which JSyCC represents MOD in what is currently a community of AUS/CAN/UK/US, from NATO. Additionally, there may be times when the CIS in question is only relevant to MOD, and so JSyCC, as an element of NISCC, will take responsibility for this dissemination rather than UNIRAS.

10. Most VWN information will be UNCLASSIFIED, as it is largely derived from Public Domain sources and then verified by NISCC / UNIRAS / JSyCC, but in some cases a protective marking may be required. In such cases, even for VWN, Signal Message dissemination will normally be used to obviate difficulties of transfer of protectively marked email to some MOD units.

Threat Information

11. The overall Information Security Threat Summary (ISTS) to MOD assets is issued on a regular basis from JSyCC to PSyA Staffs, which provides a more granular version of the Government-wide Annual Threat Assessment (ATA), including details for MOD units not within the UK mainland that the ATA primarily covers.

12. To supplement the ISTS, a dynamic system of Threat A&W Information is provided by JSyCC, based on security intelligence material collated from a number of internal and external sources.

13. The UK MOD uses the UNCLASSIFIED Codeword "CANNEL" for Overall Threat Alert levels, which are broadly equivalent to the "InfoCon" levels in use by the US Department of Defence (DOD), and a general measure of the Threat level within the static environment.

14. The meaning of the Cannel levels are given in the following table :

Cannel Level	Threshold Level	Response/Counter-Measure
White	This level is designed for when there is a general warning of possible Malicious Electronic Attack (MEA) activity.	a. Routinely monitor all Internet gateway access points for potential and anomalous activity. b. Routinely monitor all audit logs as required at **Chapter 12**. c. Ensure that anti-virus vendor software (AVS) is the latest version and that it is updated as required at **Chapter 8.** d. Ensure that Installation Vulnerability Reviews (IVR) are performed as required at **Chapter 12**.
Black	This level is to be used when there is an increased Threat and there is Intelligence to indicate an increased likely hood of MEA or that significant MEA is occurring in other countries and in UK/Foreign commerce. This level should be implemented under the following conditions:	In addition to the actions for White, the following responses/counter measures are required to be implemented: a. Carry out local review of physical and network security measures to ensure they meet the requirements of the Target of Accreditation.

	a. When a number of specific incidents of MEA have occurred on MOD CIS at MOD HQs, military locations or during military operations and deployments. b. Significant military operations/deployment are either planned or being conducted. c. A noteworthy pattern of scans, probes has been identified or suspected on MOD CIS.	b. Increase the frequency that audit logs are inspected. c. Review Secure Managed Interface (SMI – e.g. firewall / IDS) configurations. d. Review Anti-virus policy with up to date IDEs e. Review local Incident Handling procedures, including contact proecdures for relevant Monitoring and Reporting Centre (MRC) as laid down at **Chapter 11**. f. Review business continuity and recovery plans.
Amber	This level should be used when limited MEA have occurred and the effect of any MEA has had limited impact on operations/deployments. This level of alert may be used under the following conditions: a. There are specific Indicators & Warnings occurring; which indicate limited MEA against MOD CIS have either occurred or are imminent. b. MEA have been detected, which have had limited operational impact on military operations or deployments.	In addition to the actions for Black, the following responses/counter measures are required to be implemented: a. Isolate any MOD CIS systems, which may have been attacked. b. Cease all non-operational internet connectivity. c. Execute a 'minimise' on all MOD CIS interconnections to provide bandwidth in support of operational activity. d. Consider re-configuration, rerouting or disconnection of critical/non critical networks. e. JSyCC and MRCs assume full 24 hour manning. f. IRSTs are placed on 6-hour response time.

Red	This level should be used when there is either a general or specific MEA on MOD CIS systems, which will have a significant disruption to military operations or deployments. It should be used under the following conditions: a. There has been a wide spread series of successful MEA on MOD CIS systems, at military locations or on military operations and deployments. b. The attacks carried out will have been widespread and will undermine the MOD ability to fulfil its military commitments. c. It is more than likely that military operation will fail.	In addition to the actions for Amber, the following responses/counter measures are required to be implemented: a. Cease all internet connectivity unless sanctioned by the Defence Crisis Management Organisation (DCMO) through JSyCC. b. Sever all connections between systems at differing protective marking levels unless sanctioned by the DCMO through the JSyCC. d. IRSTs are placed on immediate on-call basis.

15. Changes to the Cannel levels are promulgated by Threat Change Notices (TCN), which are necessarily brief to ease the load on the signal system. In most cases additional information for any increased TCN will be provided in a Threat Warning Notices (TWN).

16. Cannel Level can only be assumed to be valid for the UK Mainland. Threat levels for Overseas based units and / or mobile staff should be sought direct from JSyCC, and for all operational deployments from JSyCC via PJHQ (SO1 J3 C2W).

17. Specific Threat information (e.g a hacker group known to be targetting specific types of hardware) are disseminated using TWN. Where the TWN information exceeds UNCLASSIFIED, Signal Message dissemination will normally be used to obviate difficulties of transfer of protectively marked email to some MOD units.

18. The unified Levels as published in the ATA and ISTS are used to describe Threat in TCN and TWN :

Level	Threat
Level 6	Very High
Level 5	High
Level 4	Significant
Level 3	Moderate
Level 2	Low
Level 1	Negligible

Request For Information

19. Request For Information (RFI) are issued when JSyCC has been given uncorroborated information relating to potential Vulnerabilities or, occasionally, Threats, and feedback is sought from the MOD community to increase the information available for a security intelligence assessment. This will typically relate to network based intrusions.

20. RFIs will normally only be sent to either MRCs or to System Operating Authorities known to have the capability to monitor connections to external networks. Occasionally, a wider RFI may be issued, for instance when a prevalence analysis is required for a specific virus.

Dissemination

21. The default method of promulgation of VWN and TWN is by electronic mail, either using Intranet or Internet mail services. The majority of the information is received by JSyCC through the internet, and thus internet broadcast may be found to be received faster than those on MOD intranets.

22. In order to receive A&W information, units must take action to ensure they receive both signal messages and email.

23. Signal Messages Receipt of signal message A&W alerts is a 2 stage process:

a. Check with the local or guard COMMCEN that traffic is received for the units Signal Message Address (SMA), and that this SMA is included within Address Indicator Group (AIG) 1001 ;

b. Request that the COMMCEN include the unit on the SIC Distribution List (SDL) for all traffic received under SIC 'Y3A'.

24. Email Dependant on whether intranet or internet conectivity is available, take the following action :

a. **Intranet** Send a message to CHOTS mailbox "JSyCC" requesting to be added to the A&W mailing list ;

b. **Internet** Send a message to mailto:jsycc@cert.mod.uk requesting to be added to the A&W mailing list.

25. Other methods of dissemination of A&W information will be subject to agreement between the Unit and JSyCC.

ANNEX H TO

CHAPTER 2

TERMS OF REFERENCE FOR A SECURITY WORKING GROUP

Constitution

1. The membership of a SWG will normally consist of the following as a minimum:

a. Project Manager or System Operating Authority — Chairman

b. Security Assurance Coordinator (SAC) — Secretary

c. DSSO/TLB Principal Security Adviser (PSyA) — Accreditor

d. OR Branch

e. ITSO / SSO Designate

2. Where no SAC has been appointed for a project of System or Project, the Project Management Authority or System Operating Authority is responsible for nomination of an alternative secretary.

3. In programs with a a formally constituted Accreditation Panel (AP), the Chairman of that panel will normally represent the accreditation community at routine SWG meetings. For large and complex programs with a permanently tasked SAC, the Accreditor(s) may choose to delegate their interests at routine SWG meetings to the SAC, who will then report matters requiring Accreditor consideration, endorsement or approval to the Accreditor(s), and in such cases , the Project Management Authority or System Operating Authority is responsible for nomination of an alternative secretary.

4. The following may also need to be involved in SWGs :

a. Other Joint Accreditation Authorities

b. National Technical Authorities (e.g. CESG)

c. Specialist advisors (e.g. (C)IDA for TEMPEST)

d. EC(CCII)IOCMProj

Aim

5. The Security Working Group (SWG) will provide the forum in which all IT security matters are discussed and formulated in support of the project sponsor and accreditors, including the development of Security Policy Documentation SPD, such as SSPs and SISPs.

6. The SWG reports to the Project Board during system development, or the System Operating Authority thereafter.

Responsibilities

7. As a minimum, the terms of reference for an SWG are to include:

a. Obtaining appropriate threat assessments through the security chain of command, identifying particular vulnerabilities, and carrying out required risk analyses.

b. Providing advice and guidance on security matters to the project board and project staff.

c. Providing advice on the areas of risk analysis and risk management as they pertain to security matters.

d. Advising on the requirements for evaluation and certification.

e. Providing advice on the implementation of security policy, requirements and proposed solutions.

f. Providing advice to project staff on the security implications of any proposed changes to the configuration, operational requirements or protective marking level of the information.

g. Reviewing and providing advice on security documentation.

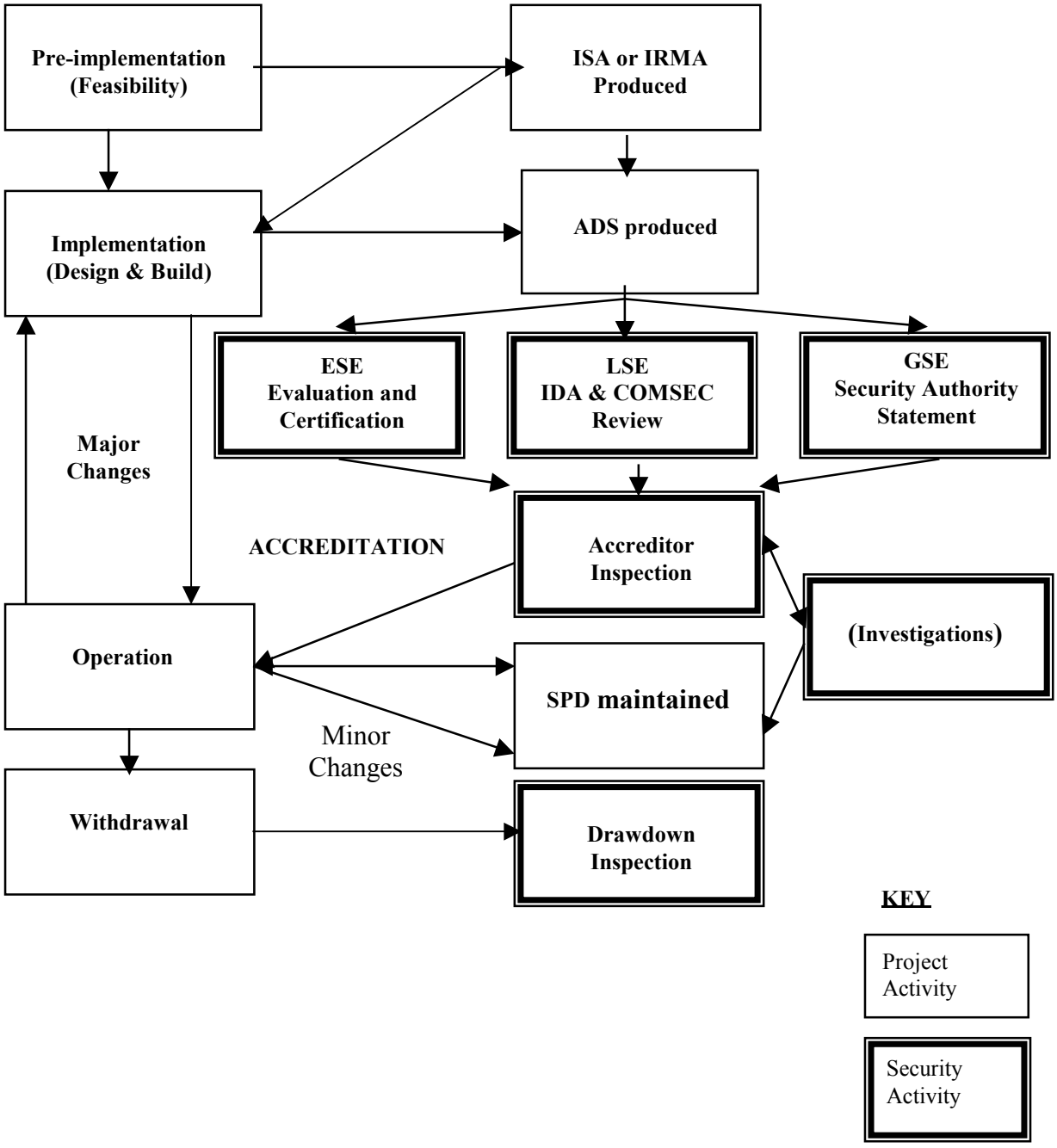
Meeting Frequency

8. The frequency of meetings shall be at a period as appropriate for the system or project concerned, but should normally be at least 2 per annum, as if less are found to be required it may be that the SWG is not really necessary.

ANNEX I TO

CHAPTER 2

THE ACCREDITATION PROCESS



This page intentionally left blank.

APPENDIX 1

ANNEX I TO

CHAPTER 2

OUTLINE FULL OR INTERIM ACCREDITATION CERTIFICATE

Ministry of Defence
Certificate of CIS Security Acreditation

<Organisation Crest>

System/Project Name	
Date of Certificate	

Reference: JSP440 (Defence Manual of Security) Volume 3 (CIS)

An Accreditation Review for this <system/project> has been carried out by the Accreditor, taking consideration of the Accreditation Evidence Statement (AES) of <date> attached.

The Residual Risks associated with <system/project> were found to within the tolerance allowed by National and Departmental Standards, and Accreditation is therefore granted.

Operation of the system outside the parameters laid down in the Security Policy Documentation (SPD) and the AES will invalidate Accreditation.

This accreditation is liable to periodic review, and a revised AES must be submitted every <x> years.

Any Significant Security Incidents, or Compliance Recommendations of Grade B or worse, must be notified immediately to the Accreditor, who reserves the right to require re-Accreditation as a result.

Accreditor Details

Name	
Post	
Representing	<TLB name or DSSO>
Signature	
Date	

Operational Authorisation

Name	
Post	
Representing	
Signature	
Date	

APPENDIX 2
ANNEX I TO
CHAPTER 2

OUTLINE CONDITIONAL ACCREDITATION CERTIFICATE

Ministry of Defence
Certificate of Conditional Accreditation:
Statement of Residual Risk Acceptance

<Organisation Crest>

System/Project Name	
Date of Certificate	

Reference: JSP440 (Defence Manual of Security) Volume 3 (CIS)

An Accreditation Review for this <system/project> has been carried out by the Accreditor, taking consideration of the Accreditation Evidence Statement (AES) of <date> attached.

The Residual Risks associated with <system/project> were not found to be within the tolerance allowed by National and Departmental Standards, and the operation of the system is therefore carried out on the basis of Risk Acceptance by the Security Champion(s) as detailed below:

Risk Area	Residual Risk	Status
Organisation & Management		<Accept/ Transfer / Mitigate>
Physical Security		<Accept/ Transfer / Mitigate>
Personnel Security		<Accept/ Transfer / Mitigate>
Media Security		<Accept/ Transfer / Mitigate>
Procedural Security		<Accept/ Transfer / Mitigate>
InfoSec – CompuSec		<Accept/ Transfer / Mitigate>
InfoSec – ComSec		<Accept/ Transfer / Mitigate>
InfoSec – RadSec		<Accept/ Transfer / Mitigate>

Operation of the system outside the parameters laid down in the Security Policy Documentation (SPD), AES, and this RRA will invalidate Accreditation.

This accreditation is liable to periodic review, and a revised AES must be submitted every <x> years.

Any Significant Security Incidents, or Compliance Recommendations of Grade B or worse, must be notified immediately to the Accreditor, who reserves the right to require re-Accreditation as a result.

Accreditor Details

Name	
Post	
Representing	<TLB name or DSSO>
Signature	
Date	

Residual Risk Acceptor (Security Champion) Details

Name	
Post	
Representing	<TLB name or DGInfo>
Signature	
Date	

SECURITY POLICY DOCUMENTATION

CHAPTER 3

SECURITY POLICY DOCUMENTATION

Introduction

0301. This Chapter gives guidance on the production of Security Policy Documentation for Communications and Information Systems (CIS) in use within Defence. This has been subdivided into 2 major elements:

a. Security Policy Documentation for small systems, which is based upon a philosophy of simple Registration provided that the generic documentation provided in Annexes to this Chapter can be complied with;

b. Security Policy Documentation for large and distributed systems, which will have to be specifically written for each CIS in question.

0302. The Manual of Protective Security requires that accreditation is achieved under the conditions specified in an Accreditation Document Set (ADS). HMG Infosec Standard No 2 provides a guide to organising and producing an Accreditation Document Set to form the basis for accreditation and the maintenance of accreditation status. The Security Policy Documentation described in this chapter fulfils the requirements of HMG Infosec Standard No 2 and a cross-reference table is provided at **Annex A**.

The Threat

0303. The origins and nature of the threats to official information processed electronically, are similar to those to protectively marked information stored and handled in other forms, which are outlined in other volumes of the Defence Manual of Security. The main threat to official information processed/stored on IT Systems is from personnel who may be from or influenced by foreign intelligence services (FIS), or authorized users who, for whatever motive, may seek to gain access to official information they have no 'need to know'. The threat from subversive or terrorist organisations, investigative journalists and others must also be considered.

0304. A general statement of the threats to the compromise of official information held in IT systems is at **Annex B** to this Chapter.

Registration

0305. **General.** In order to standardise IT registration procedures, within the MOD, the use of a common form will be necessary. The form is given at **Annex C**. It is to be completed by the system/installation manager when the IT equipment/software is received within their area of responsibility. Once completed the form should be retained

by the manager and a copy sent to the ITSO/ESyO. As and when there is an amendment to be made to the document the manager must notify the security authorities accordingly.

a. **Hardware.** When a new IT system is received the system/installation manager will record, on the Registration Form, all the details required ensuring that serial numbers etc are correct. The completed form will then be forwarded to the appropriate branch/unit security officer. When IT equipment is replaced or disposed of details will be notified to the security officer. If at any stage of the systems life-cycle the equipment is moved from its approved location the system or installation manager will record details on his copy of the Registration Form.

b. **Software.** When the system/installation manager takes delivery of a new IT system he will record on the Registration Form details of all software supplied with that system. Details will include the name of the operating system and any applications software that is supplied by the manufacturer/distributor of the system. Details of the software licence number and the date installed will be recorded on the Registration Form. If at any stage in the future additional software is loaded and stored on the system the Registration Form is to be amended accordingly by the ITSO. This recording action will assist in identifying any unauthorized software that may be resident on the system.

Documentation Requirements – Small Systems

0306. Generic SyOPs for stand alone PCs operating in the dedicated mode are at **Annex D**. (Generic SyOPs for portable IT systems operating in the dedicated mode are included in **Chapter 8**.) When completed the SyOPs may be forwarded with the registration form (Annex C) and a covering letter in the format of Appendix 1 to Annex C to the accreditor for approval. This obviates the need for system specific Security Policy Documentation.

0307. An outline of the Security Policy Documentation for small systems (small Local Area Network (LAN) or Server with several terminals) is at **Annex E**. **Annex F** is a guide for the production of SyOPs for systems other than standalone PCs or portables.

0308. For unclassified systems, the security statement may do no more than to ensure that the system is not used for protectively marked information. The relevance of the Data Protection Act, other legislation, protection against unauthorized amendment or system denial (e.g. by virus attack) will need to be considered, as will interconnections to other systems.

Documentation Requirements – Large and Distributed Systems

0309. The MOD has adopted a "portfolio" approach to the production of Security Policy Documentation aimed at producing a number of small well-focused items, rather than the monolithic and cumbersome documents that had been used in the past. The intention is both to reduce duplication of effort, and minimise the amount of nugatory reading required.

0310. Under the portfolio approach, Security Policy Documentation for large and distributed systems may be produced for one of 2 reasons:

a. As part of the Project Management cycle, often dealing with Project and Infosec Risk. These documents normally have a title beginning with “Infosec";

b. As part of the Accreditation Document Set, which provides the evidence to support an accreditation. The evidence requirements will be documented in an Accreditation Evidence Statement (AES), which could include Legacy Documentation (see para 343) in addition to the new Security Policy Documentation defined in this chapter.

0311. Several of the new documents specified in this chapter are derived from the Domain Approach research, conducted under the MOD’s Applied Research Programme. Additional guidance on these documents will be incorporated into Defence Information Assurance Notice No. 7, ‘Security Policy Documentation’.

0312. **Accreditation Certificate**. Unlike small systems, where a countersigned Registration Document acts as the proof of compliance requirements for Security Policy Documentation production, and the CIDA Conformance Certificate **(Chapter 20**) provides evidence of correct installation, large and distributed CIS will have a dedicated Accreditation Certificate, issued by the Accreditor(s), stipulating the Accreditation Conditions. This will be **countersigned by the System Operating Authority as accepting any residual risks.**

0313. D Def Sy can provide an example of an Accreditation Certificate. In some case this may be issued by other means (e.g. letter or signal), with the System Operating Authority’s confirmation of receipt and acceptance or conditions and risks completing the Certificate.

Project Documentation

0314. Project Documentation shall consist of:

a. Project Registration Form (PRF);
b. Infosec Scoping Appraisal (ISA).

0315. Project Documentation may also include the following:

a. Infosec Risk Management Appraisal (IRMA);
b. Infosec Management Plan (IMP).

0316. **Project Registration Form (PRF)**. The PRF acts as the initial Registration with the Accreditor(s), and must be completed for all systems other than those small systems using generic documentation. It is intended to allow forward planning of Accreditor resources to support projects. A sample is given at **Annex G**.

0317. Projects, which are sufficiently complex to warrant the raising of a PRF will also need to raise a CIDA Notification Form (CNF), details of which are provided at JSP480 – Code of Practice for Installation Design.

0318. **Infosec Scoping Appraisal (ISA)**. An ISA documents the results of an appraisal of the security-related risk to a project or group of related projects. An ISA should be short, generally no more than 6 pages of information, and for simple projects may be as little as 1 page. A template for an ISA is at **Annex H**.

0319. The purpose of conducting the appraisal is to minimise the risks to the project(s) arising from the need for security controls and accreditation. It should be concerned in broad terms with the security aspects of the requirements and the risks associated with them. Although some consideration of possible solutions will need to be made, the overall emphasis should be on identifying security-related risk to the project(s) and managing the accreditation process. An ISA shall include the Security Risk Category for the project(s), see **Chapter 14**.

0320. All new projects shall produce an ISA. The ISA shall be endorsed by the accreditor(s) before any significant budgetary commitment to the project. Note that an ISA does not form any part of the evidence supporting the accreditation decision(s).

0321. **Infosec Management Plan (IMP)**. An IMP is an overall plan for managing the accreditation process for a project or set of related projects. Further details about the expected contents of an IMP are given in **Annex I**. An Annex to the IMP should contain the Accreditation Evidence Statement (AES) for each planned accreditation decision.

0322. **Accreditation Evidence Statement (AES)**. An Accreditation Evidence Statement (AES) is produced by the Project Management Authority as a summary of progress against the main activities identified within the IMP, and is used to prove to both the Accreditor and System Operating Authority that the system is fit for purpose. Once the system is accredited, the AES is to be annexed to the Accreditation Certificate.

0323. In endorsing this implementation the Accreditation Authorities assume that the information supplied is accurate. The inclusion on this system of data in categories and protective marking levels not covered in this document, or connection to external systems, without the prior written permission of the Accreditor(s) shall be sufficient to instigate security breach investigation procedures. Further details about the suggested structure of an AES can be found at **Appendix 1 to Annex I**.

0324. **Infosec Risk Management Appraisal (IRMA)**. An IRMA records the options for the Target(s) of Accreditation that have been considered, identifies which one will be taken forward and justifies the decision. In order to reduce the risk that the proposed security solution is unaccreditable, technically infeasible or

operationally ineffective, it should be agreed between the accreditor, project and user community. Further details about the suggested structure of an IRMA can be found at **Annex J**.

Accreditation Document Set

0325. An Accreditation Evidence Statement (AES) shall define the required contents of the Accreditation Document Set for a specific Target of Accreditation. An Accreditation Document Set may contain any of the following documents, and may also include legacy documentation, (see para 343):

a. Security Risk Assessment (SRA);
b. Security Requirement Statement (SRS);
c. Security Aspects of the Design (SAD);
d. System Configuration Model (SCM);
e. Code of Connection (CoCo);
f. Interconnection Security Measures Statement (ISMS);
g. Operational Security Management Plan (OSMP), which includes a number of separate Security Operating Procedures (SyOPs) as free-standing Annexes.

0326. **Security Risk Assessment (SRA)** A SRA records the risk assessment for a specific Target of Accreditation, and further details about the expected contents of a SRA are given in **Annex K**. **Chapter 14** gives generic guidance on Risk Assessment and Risk Management.

0327. **Security Requirements Statement (SRS**) A SRS defines the detailed security requirements for a Target of Accreditation against which the effectiveness of the implementation can be assessed as the basis for accreditation. Further details about the expected contents of a SRS are given in **Annex L**.

0328. The SRS includes non-technical aspects, such as physical and security management requirements, and the requirements for security barriers, security functionality and evaluation assurance. The risk assessment, which justifies the requirements in the SRS, should be recorded in the SRA. Note that an early version of the SRS may be used to support the ITT for a development contract.

0329. **Security Aspects of the Design (SAD)** A SAD describes how the design and implementation of the system meets the requirements defined in the SRS. Further details about the expected contents of a SAD are given in **Annex M**. Note that the response to an SRS in an ITT may be an Outline SAD.

0330. **System Configuration Model (SCM)**. The SCM is the living document used to record the current configuration of the system, reflecting changes as they occur to ensure that a valid baseline for both internal and external compliance checking activity is available. **Annex N** provides an outline of the type of information that

should be contained in a SCM, although it is likely for larger systems that the SCM will be held in a database rather than as a monolithic hardcopy document.

0331. **Code of Connection (CoCo)**. Further details about the suggested structure of a CoCo can be found at **Annex O**. Where only a bilateral connection is ever envisaged, a short Interconnection Security Measures Statement (ISMS) can be used instead.

0332. **Interconnection Security Measures Statement (ISMS)**. The Interconnection Security Measures Statement (ISMS) are used where only a bilateral connection is ever envisaged, and thus a CoCo would be inefficient. Further details about the suggested structure of an ISMS can be found at **Annex P**.

Operational Documentation

0333. Once a system has been designed and implemented, an **Operational Security Management Plan (OSMP)** is required to support the Installation, Commissioning, Operation and Withdrawal of the CIS. An OSMP shall contain, or refer to, all the information necessary to configure, operate and maintain the Target of Accreditation in a secure manner. Further details about the expected contents of an OSMP are given in **Annex Q**. This includes the SyOPs, roles and responsibilities and re-accreditation conditions. OSMPs are required to be maintained throughout the system lifecycle. An OSMP should include:

a. Installation and Commissioning Security Instructions (ICSyI);

b. Technical Operation and Maintenance Security Instructions (TOMSyI);

c. User Security Instructions (USyI) or Subscriber Security Instructions (SSyI);

d. Incident Response Plan (IRP) - template at **Appendix 1 to Annex Q**;

e. Emergency and Contingency Plan (ECP) - template at **Appendix 2 to Annex Q**.

0334. The OSMP will need to be updated to reflect changing staff responsibilities, and the Emergency and Contingency Plan (ECP) and Incident Response Plan (IRP) will need to be regularly tested.

0335. A guide to the production of Technical Operation and Maintenance SyOPs for UNIX based systems is at **Annex R** to this Chapter and much of it may also be relevant to production of SyOPs for other operating systems used for medium and large systems.

0336. SyOPs are to be produced to the satisfaction of and for approval by the Accreditor, whose decisions on the SyOPs are final. SyOPs are the documentation/orders specifying the procedures, which are to be, carried out in order to ensure the security of a system as defined in the Security Policy Documentation.

0337. The use of all Departmental CIS facilities is, and will continue to be, subject to monitoring. All material held on MoD CIS equipment is deemed to be the property of the Department itself, and staff are reminded that, as a consequence, so-called "private" information held on any Departmental IT facility will not be afforded any special protection and will be accessible to line management and investigating staff without prior recourse.

0338. All SyOPs shall include the statement in the previous paragraph. SyOPs shall also ensure that the users recognise that in signing the Security Operating Procedures (SyOPs), they assent to such monitoring and implicitly indemnify the MOD against any action under Article 8 of the European Convention on Human Rights.

Maintenance

0339. Once in service, in order for the Accreditation Document Set to continue to be relevant, it is import that the System Operating Authority arrange for all Security Policy Documentation to be reviewed at least annually, and at any major change in the Environment (technical or physical).

Compliance

0340. **System Documentation**. The production of Security Policy Documentation is a prerequisite to the achievement of System Accreditation, as laid down at **Chapter 2.**

0341. As part of the Verification Activities laid down in **Chapter 12**, checks will be performed on all operational systems to ensure that the Security Policy Documentation in use is both available and still relevant.

0342. **User Documentation**. In order to demonstrate that users are conversant with the Security Operating Procedures (SyOPs) that affect their particular function, ITSOs or their delegated representatives should maintain a log showing which SyOPs have been provided to each users. Users should be required to regularly re-sign that they are aware of the SyOPs requirements.

Legacy Documentation

0343. National guidance on the production of System Security Policies (SSPs), and associated Security Policy Documents, is set out in CESG Electronic Information System Security Memorandum No. 5 ("Memo 5"). The main Security Policy Documentation items that were required by the Memo 5 were:

a. PSP – Program Security Policy;
b. CSP – Community Security Policy;
c. SSP – System Security Policy;
d. SEISP - System Electronic Information Security Policy;
e. SISP - System Interconnection Security Policy.

0344. All of the above may be found prefixed with an "I" to indicate the Initial version, as the development approach was one of reiteration, frequently leading to large and cumbersome documents with much redundancy. To aid those encountering such documents, or charged with maintaining such Security Policy Documentation for Legacy systems, the following guidance may be helpful.

0345. **Community Security Policy (CSP).** A CSP is a high level document that brings together the common security requirements of a family of related CISs. The SSP of each CIS in the family will be based on the CSP. CSPs are part of the accreditation process and are produced by, or on behalf of, the Project Manager to the satisfaction of, and for approval by, the accreditor.

0346. **System Security Policy (SSP).** The SSP under Memo 5 documentation forms the basis for accreditation. It should be prepared by, or on behalf of, the Project Manager to the satisfaction of and for approval/endorsement by the Accreditor. The Accreditor's decisions on SSP matters shall be final. In order to establish that the operation of an CIS will not breach security, the Accreditor will require an explicit statement covering:

a. The scope of the system (a brief system description or schematic).
b. The protective marking of the information to be processed, stored or forwarded.
c. The specific measures that are to be implemented.
d. The allocation of responsibilities for enforcing them.
e. Any appropriate measures that the Accreditor may deem necessary.

0347. This information was set out in a formal document, known as the SSP. A SSP was required for all CIS processing official information. The introduction of CIS and other electronic systems can cut across the normal chains of responsibility within a unit or HQ and it is a purpose of the SSP to clarify such issues and, in particular, to establish overall responsibility for system security. To this end the scope of the system is defined in terms of managerial responsibility. The SSP is a dynamic document. It can be amended to meet changes in the system, only with the approval of the accreditor.

0348. It should be noted, however, that Memo 5 is written to cover the general case for all Government CISs, and as a result it may prove difficult to apply in practice. Nevertheless the guidance set out in Memo 5 is valid. It does require interpretation, tailoring to meet specific situations and a clear understanding of both the users needs and the technical proposals.

0349. **System Interconnection Security Policy (SISP).** The SISP is essentially a memorandum of agreement between two or more System Managers on the security aspects of an interconnection between their systems, and provides a basis for accreditation. SISPs are to be produced to the satisfaction of and for approval by the Accreditor.

ANNEX A TO

CHAPTER 3

THE ACCREDITATION DOCUMENT SET (FROM HMG INFOSEC STANDARD NO. 2)

1. This Annex provides a mapping, for those familiar with HMG Infosec Standard No. 2 (IS2), of the information required by IS2 to the documentation that will be used in MOD. Details of the MOD documentation set are contained in Chapter 3 (Security Policy Documentation).

	IS2 Item	**MOD Equivalent**
Part 1 (Core Items)	Accreditation Scope	Accreditation Evidence Statement (AES)
	Links and Dependencies	Operational Security Management Plan (OSMP)
	IT Resources	
	Security Personnel	
	Compliance and Re-accreditation	
	Business functions	Security Requirements Statement (SRS)
	Asset Valuations	
	User Groups	
Part 1 (Supplementary Items)	Asset Register and values	

Part 2 (Core Items)	Countermeasures	Security Aspects of the Design (SAD)
	Risk Management Summary	Security Risk Assessment (SRA)
	Technical Risk and Assurance Requirements	
Part 2 (Supplementary Items)	Risk Register	
	Risk / Boundary / Countermeasure cross-reference	
	Risk Management Statement	
	Waiver Acceptance Form	

	IS2 Item	MOD Equivalent
Part 3 (Core Items)	Security Operating Procedures (SyOPs)	Operational Security Management Plan (OSMP)
Part 3 (Supplementary Items)	Accreditation Management Plan	
	Interconnection Security Measures	Security Aspects of the Design (SAD), Annex(es)

Part 4 (Core Items)	Accreditation Certificate	Accreditation Certificate
Part 4 (Supplementary Items)	Inspection Reports	Verification Activity Reports
	Incident Reports	GS490

ANNEX B TO

CHAPTER 3

STATEMENT OF GENERIC THREAT

Introduction

1. The origins and nature of the threats to information processed electronically are similar to those for information held in other forms. This statement concentrates on aspects in which the threats to information which are particular to Information Technology (IT). It does not consider the risks from hazards such as fire or flood. In particular it does not give advice on specific counter-measures which should be implemented as a result of a vulnerability and risk assessment for a given system.

2. This statement covers the general threat to IT systems. In special situations (e.g. Northern Ireland) a specific threat assessment should be obtained through the security chain of command.

Origins Of The Threat

3. **Foreign Intelligence Services.** The collection of Defence, Scientific, and Technical information is a high priority for Foreign Intelligence Services (FIS). The increased use of IT to process, store, and distribute large quantities of protectively marked information, including critical operational data, will make IT systems an attractive target for FIS, and it is likely that they will seek ways of exploiting any security weaknesses which they discover. Nevertheless, FIS are likely to be inhibited from carrying out operations against IT systems by the difficulty of obtaining adequate access in a hostile environment and, in peacetime, by the risk of discovery and consequent embarrassment. The threat from FIS may rise significantly during the early stages of Transition to War (TTW), but will fall after the withdrawal of diplomatic and trade missions prior to the outbreak of war.

4. **Subversive Organizations and Individuals.** Subversive organizations are often opposed to the use of IT by the State and may exploit opportunities to penetrate and disrupt them. There is, however, no evidence that any subversive group or individual has sought to acquire protectively marked information from IT systems or has the resources to mount a technical attack. Sabotage is the most likely form of attack if any easy opportunity is presented, especially in mainland Europe.

5. **Members and Sympathizers of Terrorist Groups.** The international elements which pose a threat to British interests include state sponsors of terrorism and individual terrorist groups. They might have an interest in acquiring specific information perceived by them to be of direct relevance to their interests. The difficulty that they would have in obtaining access to IT systems holding protectively marked information would, however, be likely to deter them from deploying resources to this end. Such information might, though, be of interest to them should it become easily accessible.

6. **Authorized Users.** IT systems are particularly vulnerable to persons who, as authorized users of terminals, may for whatever reason endeavour to disrupt the system or to obtain information which they may have no 'need to know'. Such persons may range from the merely curious, through those who have a grudge, to agents of FIS. Experience has shown that at least half the attempts to hack into systems arise from this group and that external hackers use "social engineering" techniques to trick authorised users into revealing information which may aid an external penetration.

7. **The Media.** Investigative journalists are increasingly interested in State IT systems, particularly those operated by the police and the Security and Intelligence agencies. There has been evidence of premeditated attempts to acquire protectively marked information from IT systems.

8. **Members of the Public.** The fact that information held electronically may be open to novel forms of surreptitious attack provides a special attraction to certain individuals, commonly known as 'hackers'. Whilst the efforts of hackers are unlikely to be directed specifically against protectively marked information, there is added kudos in breaking into Defence systems, so much information might be discovered fortuitously. This threat is enhanced by the spread of computer literacy and the publicity given to the use of "Internet" and similar data services. In particular there is a high threat to any unprotected IT system connected to the public telephone network.

9. **Theft and loss and capture.** There is ample evidence that IT hardware and components are attractive targets for theft by the criminal community. The small size of modern portable computers, and in particular storage media associated with IT systems, have frequently led to loss. For operational systems the risk of capture has to be assessed.

Methods Of Attack

10. **Agent Penetration.** As with information held in other forms, the most likely method of attack on electronically-processed protectively marked information is through an agent within an organization who has legitimate access either as a user or as an IT specialist, such as an engineer or programmer. Apart from seeing, copying, or otherwise procuring protectively marked information, an agent may be able to subvert system

security by modifying or circumventing the software or hardware controls to allow unauthorized disclosure, corruption, or destruction of the information. The growing use of computer networks presents particular opportunities for this form of attack. It is even possible for a specialist agent to set up means for an attack (for example through software modification), which will lie dormant until activated by a person or event at a later date; possibly long after the agent has left his job. The uncontrolled use of remote diagnostic facilities may also create opportunities for attack, especially when conducted from outside the United Kingdom.

11. **Malicious Software.** A range of malicious techniques have been developed to exploit the vulnerability of computer software to unauthorized or unknown modification. The boundaries between different types of malicious software are not always clear-cut, but generally they fall into one or more of the following: viruses; Trojan horses; logic bombs; worms and mobile code. Malicious software is now widespread and the speed of infection is increased by the use of interconnected and distributed systems.

12. **Interception and TEMPEST.** Like all communications links, data links are vulnerable to interception, particularly when transmitted by radio relay. Most long distance communications involve radio relay links. In addition, many types of electronic equipment emit unintended information-bearing radiation (TEMPEST), which may also be detected. The TEMPEST threat in the United Kingdom is generally Very Low except for some sites in the Greater London area. In North-West Europe and in other Commands, where sites can be in close proximity to foreign diplomatic premises or ships, the threat is higher.

13. **Terrorism and Sabotage.** The controlled operating environment required by mainframe computers make them vulnerable through the disruption of essential services such as air-conditioning, and most IT hardware is itself fragile. A terrorist or sabotage attack could therefore result in denial of service and the incidental loss or damage of information; there is however no evidence that any group has ever considered mounting such an attack specifically against protectively marked information. In TTW and war, sabotage teams may be expected to operate.

14. **Network Penetration.** The technical expertise available to FIS and the criminal hacker community is high and probably exceeds other groups. It does not preclude such expertise being purchased. Such hackers will target defence systems, and in particular those with little or no security protection in the hope of collating aggregated information. They will make use of "social engineering" (lying, normally over the telephone) to obtain background information before mounting an attack. Even if their activities do not lead to compromise by unauthorised disclosure of information, they may well corrupt or delete critical parts of system data or software.

Conclusion

15. The main threat to the compromise of protectively marked information on IT systems comes from authorized users who may, for whatever motive, disrupt the system or gain access to protectively marked information which they have no 'need to know'. There is also a threat from FIS, which are likely to try to exploit any security weakness of which they become aware . The threat from subversive and terrorist organizations, criminal activity, investigative journalists, and members of the public cannot be discounted.

16. **Malicious software.** Computer viruses and other forms of malicious software can be introduced into an IT system in a number of ways including carelessness or through malicious intent. Regardless of the way that Malicious software is introduced the effects can be severe. Macro viruses are spread by both floppy disk and E-mailed attachments.

ANNEX C

RESTRICTED
(When Completed)

CIS SECURITY REGISTRATION DOCUMENT

To be completed in typed format - 1 copy to be forwarded to Branch/Unit Security Officer

UNIT NAME:	**SYSTEM REGISTRATION NUMBER:**
COMPUTER MAKE:	**MODEL:**
SYSTEM NAME:	**DATE INSTALLED: / /**
LOCATION OF EQUIPMENT	**SYSTEM SPONSORS:**
IS SYSTEM TEMPEST COMPLIANT? Y/N (FOR SYSTEMS PROCESSING CONF AND ABOVE) **DATE AND REF OF TTA:**	**DATE OF CLEARANCE: / /**
MODE OF SECURE PROCESSING: (DEDICATED/SYSTEM HIGH/MULTI-LEVEL COMPARTMENTED)	**HIGHEST PROTECTIVE MARKING OF DATA PROCESSED TS/S/C/R/U**
IS CAVEAT, CODEWORD OR IDO DATA BEING PROCESSED?:	
TYPE OF SYSTEM: (MAINFRAME/MINI/MICRO/PC/WP/LAPTOP/OTHER):	
STANDALONE OR NETWORK SYSTEM:	
BRIEF DESCRIPTION OF SYSTEM FUNCTION AND ROLE:	
IF PERSONAL DETAILS RECORDED ON SYSTEM, IS SYSTEM REGISTERED UNDER THE DATA PROTECTION ACT? (Y/N) **DATE REGISTERED: / /**	
STORAGE MEDIA USED (FLOPPY/TAPES/DISKS/STREAMER/OTHER): **(STATE IF FIXED HARD DISK INSTALLED) SIZE ..... MB**	
ON-SITE COMMUNICATIONS (COPPER/FIBRE-OPTIC/ENCRYPTION):	
TYPE OF EXTERNAL LINK (IF ANY): **(PRIVATE WIRE/DIAL-UP/ENCRYPT).** **HIGHEST PROTECTIVE MARKING OF DATA BEING TRANSMITTED:**	
NAME OF OPERATING SYSTEM USED	

LIST OF IT EQUIPMENT AND SOFTWARE

Ser	Manufacturer	Type/Model/Version	Licence No/Ser No	Remarks/Date in use

APPENDIX 1 TO

ANNEX C TO

CHAPTER 3

OUTLINE LETTER TO BE SENT TO ACCREDITOR

REQUEST FOR ACCREDITATION COMMUNICATIONS & INFORMATION SYSTEMS

Reference:

A. JSP 440 Vol 3 - Defence Manual of Security - Information Technology
B. Data Protection Act 1984 and Data Protection Act 1998.

1. In accordance with Reference A, authority is sought to operate the IT system whose details are listed in the attached registration proforma.

2. In accordance with Reference B; .....
[at this point insert a statement as to whether the system does or does not hold personal data; whether it has or has not been registered; or if the system is exempt and the registrar informed].

3. Advice has been given for TEMPEST control and this advice has been incorporated for this installation.

4. It is understood that no alteration may be made to the system once it has been accredited.

Signature
Rank
ESyO/ITSO
Tel extn:

System Accreditation

1. SyOPs seen and approved by:

Name .....…… Appointment .....……. Date .....…..
Signature:-

2. System accredited by:

Name .....…… Appointment .....……. Date .....……
Signature:-

(Original to be returned to the originator and a copy to be retained by the accreditor.)

ANNEX D TO

CHAPTER 3

STANDALONE PCS GENERIC USER SECURITY OPERATING PROCEDURES

Introduction

1. This document constitutes the System Policy Documentation (SPD) and the Security Operating Procedures (SyOPs) for the IT system, when read in conjunction with the attached registration form. They are issued by the ITSO in accordance with Defence Manual of Security Volume 3, and have been approved by the Accreditor. All personnel using the systems are to comply with these SyOPs, and no departure from or amendment to them is permitted unless prior authorization is obtained from Accreditor.

2. Breaches of these orders may render the offender liable to disciplinary action.

Administration And Organisation Of Security

3. The appointments of IT Security Officer (ITSO) and Installation Manager (IM) relating to this system are given in the attached Annex to this document. Direct access to each installation is limited to those personnel listed by the ITSO as being approved users, who must have signed as having read and understood these SyOPs before commencing processing, and must subsequently sight them at least twice annually.

4. The term user throughout these orders refers to the Authorised User of each equipment who is cleared to see and process any information on their own equipment

5. The highest protective marking of material which may be held or processed on this system is: ..... Systems are only approved for the processing sessions and protective markings of material as specified in the registration form.

Physical Security

6. The system may only be used in the location(s), as specified in the Registration form, and may not be removed without the permission of the ITSO, after consultation with the Installation Design Authority (IDA)/Coordinating IDA (CIDA), Accreditor, or their delegated representatives.

7. When not in use all removable media, which includes Printer Ribbons (where appropriate), as well as magnetic media such as floppy disks and removable hard disks, must be securely stored in a container appropriate to their protective marking. It is to be remembered that magnetic media will assume, and are to be colour coded for, the highest protective marking of information stored or processed on the system {if DEDICATED} or permitted by the session {if SESSION PROCESSING}.

8. Any keys and Personal Identification Devices (PIDs) for the computers are to be secured appropriately for the protective marking whenever the equipment is not in use.

9. The printer is to always be checked and cleared of any printed output before the office is left unattended. Where a laser printer has been used to print PROTECTIVELY MARKED documents, an UNCLASSIFIED test print is to be run through the machine before switching off to clear the printer memory.

10. VDUs and printers are to be situated so that no data can be overlooked from either outside the area, especially from outside the building, or by persons within the area who are not authorized users. In open plan offices, any 30 minute rule is only acceptable if all personnel having uncontrolled access to the area have Need To Know (NTK), and in other cases the following additional measures are needed : {eg screen blanker with password to reactivate}

User Security

11. Each user is responsible for the security of their equipment and any magnetic media associated with it or any output produced by the equipment in either paper or magnetic form and the protection of any password.

Document Security

12. All magnetic media is to be uniquely marked and registered in accordance with Security Regulations. Unless declassified by data destruction (See Annex C to Chapter 4) the Protective Markings of magnetic media will be retained and will determine the eventual method of disposal of the media.

13. All printed material is to show the protective markings of the information, marked in accordance with the security regulations and the procedures for receipt, exchange, dissemination, declassification and destruction of such material followed accordingly.

Hardware Security

14. All equipments are to be checked before use for obvious signs of tampering. Any suspected problems are to be reported to the ITSO without delay and the equipments are not to be used until checked and cleared.

15. All protectively marked material is, where possible, to be removed from the equipment before maintenance engineers are allowed access to the equipments. Unless appropriately security cleared engineers must be supervised whilst they are working on the equipment.

16. All magnetic media introduced to the system by the engineer for diagnostic purposes must be virus checked first. All magnetic media used on the system and faulty items removed from the system must be treated in accordance with the security measures appropriate to the highest protective marking of data held on the system; this will normally result in such items being retained on Defence premises.

17. Items of equipment which may contain protectively marked material are not to be removed from MOD premises for repair without permission from the appropriate security authority. Where such permission cannot be given repair of the equipment will be by total replacement of the faulty part(s) and the damaged component(s) must be retained and destroyed in a manner commensurate with the potential protective marking. Where protectively marked data is involved any magnetic media used by an engineer for diagnostic purposes must be retained and the security measures pertaining to other magnetic media apply.

18. All hardware failures must be reported to the SM who will arrange for the necessary maintenance and maintain the records of system failures.

Software Security

19. All software used on the system is to be from authorised sources and properly licensed. Software may only be installed with the express authority of the ITSO and after the installation disks have been checked for viruses.

20. Back-up copies should be made of any software or data essential to the operation of the system. These should be kept in a different location to the working copies of the software and data files. Back-up copies should be made frequently and an annual test should be conducted to verify that the back-up copies are usable. Disks used for backing up data must be checked for malicious software before use. Once back-up disks have been made, they are to be stored at a location away from the main site.

21. Any suspected attack by malicious software must be reported to ITSO without delay and the system should not be used until a security investigation has been carried

out. #Insert after here either the full rules from DMS Vol 3 of the actions to be taken or refer to the chapters and paragraphs. This will depend on whether the machine is used solely on Defence sites.#

Communications Security

22. No other terminal, PC, modem or fax (of whatever description) is to be attached to the equipment covered by these SyOPs, and the equipment is not to be connected to a network.

Tempest Security

23. All equipment is to be installed, and the installation maintained, to comply with any requirements from BTR/01/200(3), and any TEMPEST certified equipments must be maintained appropriately.

Accounting And Audit

24. Protectively Marked information held on the IT systems is to be subject to the same degree of audit as that held by other means. Individual staff are responsible for the security of any data held on their systems. All protectively marked magnetic media will be subject to the normal mustering and spot check procedures.

Losses And Breaches

25. Any incident involving a breach of personnel, hardware, software, document, or physical security is to be reported immediately to the ITSO.

Emergency And Backup Procedures

26. Backups. Individual users are responsible for ensuring that back-up copies of any data files essential to their work are adequately maintained.

27. Emergency, Fire and Evacuation. In the event of any other incident requiring the evacuation of the area, the equipment is to be, if possible, be secured, but not at the expense of personal safety.

Virus Protection

28. Anti-virus software must be used when data are input to the system on magnetic or optical media. If CESG certified anti-virus software is available it must be used, otherwise DGICS catalogue listed anti-virus software must be used. The procedures used depend on whether the organization has implemented anti-virus 'border protection' or not. The attached annex gives the location of the anti-virus 'sheep dip' facilities if available. The following procedures must be adhered to in each case.

a. Anti-Virus Border Protection Implemented.

(1) All exchange media from outside the organization are to be checked for viruses on the supplied 'sheep dip' Pc before being used on the system.

(2) Any disk destined for a system must be checked fro viruses first.

(3) Disks from inside the organization do not need to be checked.

b. Anti-Virus Border Protection Not Implemented. 'On-access' virus protection software must be installed and active at all times. The installed anti-virus software must be updated on a regular (monthly or better) basis.

29. All users who receive a significant number of compressed or encrypted files should install 'On-access' virus protection even if they are protected by a 'Boundary Protection Facility'. The following procedures should be followed to provide additional protection.

a. All exchange media are to be write protected once prepared.

b. Unless explicit permission is given by the system manager, only data files may be copied.

c. As soon as the copy has been made, the transfer diskette must be returned to the originator. Under no circumstances is the system to be rebooted while the exchange medium is in place.

d. The system manager should change the BIOS settings to force system to look for the boot-up sector on the C: drive before looking at the A: drive.

30. If a virus attack is suspected the following actions must be taken.

a. STOP USING THE WORKSTATION AT ONCE.

b. Do not switch off or re-boot the system until being given permission to do so by ITSO or PSyA.

c. Inform the System Manager and ITSO immediately.

d. Locate and isolate all disks and other i/o media which may have been used on the infected workstation.

e. Identify and isolate any workstation which may have been infected.

f. Identify and warn any users that may have been sent infected files.

31. Recovery of data must not be started until the ITSO is satisfied that any investigation will not be compromised and gives explicit permission to begin. Virus scanning and eradication of viruses from suspect workstations and disks is only to be carried out by personnel specifically authorized to do so by PSyA.

32. Where the anti-virus strategy incorporates the use of a central 'sheep dip' facility, reinforced by the use of a workstation media authorization guard (WMAG), the WMAG package must be set for a specific protective marking level. If there are systems working at different protective marking levels, the WMAG must be set on a separate machine for each protective marking level. End user systems should not contain software capable of subverting the WMAG mechanism such as primitive level disk editors.

33. Instructions describing the treatment for electrical shock are to be displayed in every room or office containing computer equipment. All Health & Safety regulations concerning electrical equipment are to be freely available to all members of staff that use such equipment and must be observed.

ANNEX E TO

CHAPTER 3

SYSTEM SECURITY POLICY (SSP) SMALL LOCAL AREA NETWORK (LAN) OR SERVER WITH SEVERAL TERMINALS

Introduction

Basic Facts

1. **Name of System/Project.** [The acronym or short name by which the system is known.]

2. **Reference No.** [Serial number of main IT system].

3. **Location of System.** [Unit, barracks, block, room, where possible.]

4. **Reference and Date of Authority to Operate.** [This may not yet be given by the accreditor].

5. **In Service Date.**

Security Responsibilities

6. **SM.** [Appointment and telephone number].

7. **ITSO.** [Appointment and telephone number].

8. **Establishment Security Officer.** [Appointment and telephone number].

9. **Accreditor.** [Appointment and telephone number].

10. **Users.** [Appointment and branch of each user should be shown].

Status Of This Document

11. **Version Number.**

12. **Superseded Documents.**

Classified Aspects [Assigned protective marking of]:

13. **System.** [This relates to any hardware, operating software or applications software that is protectively marked. The highest protective marking for each should be shown].

14. **Description of System.** [This is the protective marking of a description of the system showing its capabilities].

System Description

15. **Role of System.**

16. Mode of Secure Processing. (Dedicated, System High Compartmented or Multi level).

Data

17. **Highest Protective Marking.**

18. **Special Category Information.** [Caveats, e.g. NATO].

Users Of System

19. **Number of Users.**

20. **Clearances.** [The lowest vetting level of the user population is to be shown].

System Configuration

21. **Hardware:**

a. Type and Make of the main IT system.

b. Number and type of peripherals. [Include all peripheral equipment, Visual Display Unit (VDU), printers, mouse, plotters, etc. Peripherals should be shown by manufacturer, model and size and quantity, e.g. Samsung 14" colour VDU qty 1].

c. Media loading arrangements. [The number and type of media loading devices should be stated, e.g. one ¼" tape drive, one 3.5" 1.44Mb floppy disk drive. The security controls for the use of these devices and the magnetic media produced by them should be detailed].

d. Hard disk arrangements. [The quantity, size and type of hard disk should be detailed as well as whether they are fixed or removable. If removable, the individual serial numbers are to be recorded. The security controls should be stated for the secure storage, registration and handling of the system hard disks].

e. Schematic diagram/Topology.

22. **Software:**

a. Proposed Operating Systems (Version Number). [e.g. MS DOS 5.0 or 6.0, UNIX 4.1 or 5].

b. Application Software. [List the application software the system is to use, e.g. WordPerfect 5,1, SuperCalc 5, etc.].

Security Arrangements

23. **Arrangements for the Secure Operation and Storage of Protectively Marked Items.** [This must include hardware, software, magnetic and paper media used by or output from the system].

24. **Maintenance Arrangements.** [The maintenance organization contracted to repair the equipment should be shown].

25. **Access Controls, Security Hardware or Software to be used.** [The minimum standards to be achieved should be shown as well as specific hardware or software security devices].

26. **Accounting and Audit Measures to be Undertaken.** [Details of the methods employed either manual or automatic]

27. **Back-up system to be employed.** [This should be a statement of the minimum requirement to recover the system in the event of failure or corruption of data. The detail of back-up procedures should be included in the SyOPs].

28. **Password system** (if required).

29. **Hardware/Software Configuration Control Procedures.** [The requirement to gain authority for any changes to hardware or software should be shown].

30. **TEMPEST Threat Assessment.** [Result of this assessment and who carried it out should be given].

31. **Limitations in use.** [The minimum spacing from other equipment including telephones and other system wiring or radio transmitters should be specified. Any special requirements that have been stipulated should be included].

Contingency Plans

32. **Fire, Flood and Serious Breakdown.** [The minimum arrangements to counteract these occurrences should be shown].

33. **Malicious Software, including viruses.** [The protective procedures to be implemented should be shown].

Accreditation Conditions

34. All requests for modification to the system must first be considered by the System Manager, who is to identify any security sensitive changes for approval by the accreditation authority. In particular no new connectivity for the system, nor any reprocessing of data in a security class for which the system is not accredited, may be made without the express approval of the accreditation authority.

35. There will be no variation from this document without the prior approval of the system accreditor.

In signing this document the accreditor assumes that the information supplied is accurate. The inclusion on this system of data in categories and protective marking levels not covered in this document, without prior written permission of the system accreditor, shall be sufficient reason to instigate security breach investigation procedures.

Accreditation Signature

.....

Accreditation Authority

ANNEX F TO

CHAPTER 3

GUIDE TO SYOPS FOR SYSTEMS THAT ARE NOT STANDALONE PCS OR PORTABLES

Introduction

1. SyOPs are a description of the method by which the security policy described in the System Policy Documentation (SPD) is to be implemented. Personnel and their responsibilities are identified.

2. SyOPs are to be produced for all systems which are intended to process or store official information. This includes word processors and electronic typewriters.

3. The ITSO should ensure that SyOPs for every system he/she has responsibility for be produced. SyOPs are required before accreditation can be given.

General Structure Of SyOPs

4. The SyOPs will address the following:

a. Administration and organization of Security.

b. Physical Security.

c. Personnel Security.

d. Document Security.

e. Computer Security.

f. Accounting and Audit.

g. Emergency and Contingency Plans.

h. Communications Security, including crypto, emission, and transmission security.

i. Configuration Management.

j. General Security Guidance to Users.

5. The content of SyOPs will vary considerably from system to system and this Annex is intended to provide guidance only. Those personnel responsible for producing SyOPs will extract from this checklist only that detail relevant to their particular system. However, the structure and content of SyOPs for a particular system must be agreed by the accreditor before security approval is given to operate.

Administration And Organization Of Security

6. This section is to contain an introduction along the lines of the following:

> "This document constitutes the SyOPs for processing official information on the ..... IT system. The SyOPs are issued by the ITSO ..... (post description) in accordance with the requirements contained in the Security Manual and in ..... (local security instructions). The SyOPs have been approved by ..... (appropriate accreditor). No departure from, or amendment to, the SyOPs is permitted unless explicit agreement from the ITSO has been obtained. Approval from ..... (appropriate accreditor) is to be obtained by the ITSO before any significant change to the SyOPs is implemented. Changes of minor detail are to be notified by the ITSO to ..... (appropriate accreditor) but are not dependent upon prior approval."

7. This section is also to contain details, where applicable, relating to the following aspects:

a. A brief description of the IT system.

b. Details of the Mode(s) of Secure Operation relevant to the IT system, and the level of protective marking permitted for each mode.

c. The security responsibilities of nominated personnel and users, including those responsible for the supervision of operations staff. A suggested form of allocation of responsibilities and duties is outlined elsewhere in this chapter.

d. Administrative procedures for the review of and changes to the list of authorized users, and access rights.

e. Extracts of communications security requirements as appropriate.

f. Procedures for the control of engineering and other support staff who may require access.

g. Procedures for protecting the system against malicious software.

h. A statement that any incident involving a breach of personnel, hardware, software, communications, document or physical security is to be reported immediately to the ITSO.

i. Instructions to ensure that SyOPs are circulated to all appropriate staff and that their receipt is acknowledged.

Physical Security

8. Physical security measures are necessary to help prevent unauthorized access to sensitive information, unauthorized operation, denial of resources, and to protect the valuable and fragile IT equipment.

9. This section is to provide details, where appropriate, of the following:

a. Definition of the computer area(s) - a floor plan of the office should be given showing the location of all IT equipment.

b. Keys and/or lock combinations - identity, where kept, records kept, who is permitted to draw and/or use.

c. Personnel (and equipment) access control:

(1) Procedures and records maintained for the control of visitors including measures applied to prevent unauthorized viewing of sensitive output or display.

(2) Passes - types in use and requirements for wearing or display of these; who is responsible for authorization and/or issue; application procedures and master records.

(3) Procedures in place to control the introduction, storage, operation, and removal of miscellaneous equipments.

d. Intruder and environmental alarms - where located, regime for testing, frequency of tests, procedures for setting alarms, and procedures for reacting to an alarm.

e. Equipment connection/disconnection instructions and procedures:

(1) Fire regulations.

(2) Hand-over procedures to be followed by the officer in charge of the shift.

f. "Two persons rule" during protectively marked processing, if applied.

g. Start-up procedures and documentation.

h. Close-down procedures and documentation.

Personnel Security

10. Any person who is able to enter a location containing IT equipment may be in a position to interfere with or damage such equipment, and have access to protectively marked material being printed or displayed. The threat to IT system security can arise from any individual who has the necessary level of professional expertise and knowledge of the system and the requisite access to the system. It follows that staff with legitimate entry to IT facilities may have unique opportunities for the unauthorized and surreptitious acquisition of information, or for permitting its extraction by unauthorized persons. In addition, there may be certain key personnel, for example systems programmers, systems analysts, and commercial consultants, with unique knowledge of the IT system security features and hence the potential to compromise them.

11. This section is to provide details, where appropriate, of all aspects of personnel security, including:

a. The personnel required, or who may be permitted, during processing periods and out-of-hours, including the appropriate minimum vetting clearances required. Where appropriate, the operation of the 'two person rule' and, where deemed necessary, as an annex to the SyOPs, a list of names of specific individuals.

b. Any specific details relating to certain key personnel - systems designers/analysts/programmers, operating personnel, commercial consultants, engineers, and other maintenance or technical staff, including, as an annex to the SyOPs, a list of names of specific individuals.

c. Security education/training requirements for all appropriate staff, including the need for formal acknowledgement of the appropriate security instructions.

d. Any specific details relating to certain ancillary staff such as cleaners and workmen.

e. Any specific details relating to who is allowed access to each site, building, room, etc.

Document Security

12. In an IT system the volume and compactness of the information processed, its ready accessibility, and the ease and speed of copying data, sometimes at remote locations, underlines the need for strict document security measures.

13. It is to be remembered that "document" covers all forms of media holding sensitive information, for example, paper documents, magnetic media, other machine-readable media, microfilm and fiche, printer ribbons, etc.

14. This section is to provide details of, where appropriate, the following:

a. All "document" types in use, including register sheets, marking conventions, and storage requirements.

b. Responsibilities and procedures for record inspection, including frequency of inspection.

c. Procedures for the acquisition, storage, and control of, and accounting for, magnetic and other machine-readable media.

d. Procedures for the receipt, exchange, and dissemination of documents.

e. Procedures for the appropriate protective marking of documents.

f. Responsibilities and procedures for the de-classification of documents.

g. Instructions relating to the disposal of redundant back-up media (where/how, at what frequency, and by whom).

h. Who is permitted access, and the access rights of these people.

Computer Security

15. Hardware and software security mechanisms can contribute separately and in combination to the security of an IT system by providing facilities for:

a. Identification of the devices, media, and users forming individual elements of the security control systems.

b. Access control whereby users are restricted to those items of hardware, software, and data to which they are permitted to have access and unauthorized access is positively denied.

c. Workstation media authorization guard (WMAG) (formerly known as floppy disk authorization guard) to prevent unauthorized use of floppy diskettes.

d. Detection and surveillance whereby unauthorized or incorrect access attempts are monitored and reported.

e. Integrity checks which give assurance as to the correct functioning of 16.a to 16.c below.

Hardware Security

16. Hardware security refers to the protective security features provided by the physical components of an IT system. This sub-section is to provide details of, or make reference to, where appropriate, the following aspects of hardware security:

a. Security-related start-up procedures and documentation.

b. Security-related close-down procedures and documentation.

c. Security-related equipment disconnection/connection instructions and procedures.

d. Procedures for the institution of regular (preferably daily) checks for signs of tampering with equipment and to ensure that hardware cabinets are kept locked in normal circumstances.

e. The computer configuration to be employed for processing under various conditions; for example, which terminals are to be disconnected and/or peripherals disabled when specific processing is to be carried out.

f. Procedures for securing the computer in preparation for engineer maintenance and repair, including:

(1) A statement of the level of authorization required for equipment modification, introduction of new hardware and software, or removal of

any item(s) of hardware, including processor boards, which may process, store, or forward official data.

(2) A statement of any restrictions imposed when scheduled maintenance may or may not be carried out.

(3) Details of any diagnostic routines to be installed either on a routine basis or following scheduled maintenance or modifications to hardware. In the exceptional circumstances that remote diagnostics or maintenance techniques have been considered and deemed acceptable by the system Accreditor, details of these, together with relevant security procedures, are to be specified.

(4) Specification of any scheduled maintenance programs including instructions for the identification of any diagnostic printout which might contain sensitive material.

(5) Procedures for the identification, storage, and control of security-related spare parts.

g. Procedures to be followed in the event of hardware failure, describing actions to be carried out, and by whom, for securing the computer at breakdown and what records of the failure are to be kept.

h. Where TEMPEST protection is provided for the system, this is to be noted and cross-reference made to the sub-section on emission security.

Software Security

17. Software security refers to the protective security features which may be provided by:

a. Microcode (or firmware) - software instructions, usually written by the hardware supplier, which simulate hardware and are conceptually replaceable by actual hardware implementation.

b. Operating system software.

c. Middleware - for example data base management systems.

d. Utility programs - providing common and frequently used facilities such as program compilation and the sorting or merging of files of data.

e. Application programs - relating to specific requirements of users.

18. This sub-section is to provide details, where appropriate, of the method of use and control of any protective features provided by software, specifying in particular the:

a. Identification (user ID) concept - procedure for allocation and deletion.

b. Authentication concept - including password control and change procedures, issuing authority, control records kept and by whom, frequency of change, and password usage procedures (covering where applicable different types of processing).

c. Access control mechanisms - the procedures for implementing discretionary or mandatory control of access to data or devices; details of the responsible authorities and control records maintained.

d. Versions of the operating system software, utility programs, software packages to be used, including any to be used in special circumstances.

e. Control over the facilities for copying or modifying the operating system software, with details of the authority and documentation required.

f. Details of precautions to be taken before and after processing or when preparing different types of sensitive work, including routines for clearing main memory, rules for de-classifying or over-writing backing store, and procedures for ensuring that buffers are cleared and that all logs and journals have been printed and over-written.

g. Integrity assurance of system software, particularly:

(1) The regeneration of the controlling system software at irregular intervals.

(2) The reloading of copies of utilities from masters at frequent intervals.

(3) The safe custody of master programs.

(4) The control/assimilation of new issues of system software.

19. This sub-section is also to provide details, where applicable, concerning system and application software, including:

a. Responsibilities for generation and use.

b. Receipt and introduction procedures, authorization and forms.

c. Protective Marking.

d. Modification/amendment and change control procedures, for all software changes (including binary repairs), authorization, and forms.

e. Copying controls.

f. Use of macros.

g. Software audit and validation procedures - what, by whom, at what frequency, and records to be kept.

h. Handling of protectively marked dumps - who is authorized to produce these, of what, for what, and records to be maintained.

i. System back-up provisions - what held, where, in what
form, what checks performed, frequency of checks, and who is authorized to set up/use these facilities.

j. Procedures to be followed in the event of a failure and records to be kept.

k. Control of hard copy (program listings, test run output, etc).

Accounting And Audit

20. The sub-section on Monitor and Audit is to be a summary of all monitoring and audit procedures, both manual and system maintained, and individual allocation of responsibilities relevant to the IT system/network. It is to include:

a. The procedures for running monitor programs and details of audit facilities.

b. Details of the security journals and how they are to be used, both for error investigation and for specific file, or personnel, oriented event or activity tracing as well as general scanning for abnormal trends.

c. The arrangements for the regular inspection of the audit trail, in order to enable unauthorized access, or attempts, to be discovered promptly and allow appropriate remedial action to be taken.

d. Responsibilities of those required to run and validate the integrity of monitor programs and undertake investigative and analysis work in the event of anomalies being discovered.

e. Details of the retention period for audit logs.

g. Procedures to be undertaken in the event of audit malfunction.

Emergency And Contingency Plans

21. This section is to provide details of the regular, security relevant, back-up procedures including, where appropriate:

a. Details of operating methods.

b. Frequency of back-up.

c. Transmission and storage requirements.

d. Procedures for access to, and use of, back-up copies.

22. This section is also to provide details of, or refer to, the security procedures, including emergency destruction procedures and those pertaining to recovery, to be followed in the event of exceptional circumstances, for example:

a. Hardware failure, software failure, or the discovery of the introduction of malicious software (e.g. virus).

b. Communications links failure.

c. Power fluctuations, or power failure.

d. Smoke, fire, or explosion.

e. Subversion, sabotage, terrorism, civil disorder, or bomb threats.

f. Flood/liquid leakage.

g. Building structure problems.

h. Earthquakes, hurricanes, and other natural disasters.

23. This section is also to provide a summary of, or refer to, the exercising of emergency and contingency procedures, and the frequency with which exercises take place.

Communications Security

24. Communications security is concerned with the protection of sensitive information being processed by, or forwarded through, telecommunications systems and can support integrity of communications services and access control through key management. It includes three specialized aspects:

a. Crypto security - defence against crypto analysis.

b. Emission security (TEMPEST).

c. Transmission security - defence against traffic analysis.

25. IT systems, including networks, which are communicating sensitive information require protection against unauthorized access resulting from communications vulnerabilities.

Crypto Security

26. This sub-section is to provide details of, or make reference to, the following aspects, of crypto security where appropriate:

a. A clear statement of who is responsible for implementing and controlling procedures for crypto security.

b. Details of the communications security (COMSEC) officer (for example, job title, and responsibilities) for those systems which use cryptographic equipment as system components.

c. Specific procedures for the use of cryptographic equipment, especially the management of cryptovariables.

d. Procedures for the re-connection of remote terminals which have been disconnected for security reasons.

Emission Security

27. This sub-section is to provide details of, or make reference to, the following aspects, where appropriate, of emission security:

a. A clear statement of who is responsible for implementing and controlling procedures for emission security.

b. Procedures for the review of TEMPEST requirements, for the facility or facilities involved, with the appropriate TEMPEST authority.

c. Procedures for the control of where portable and standalone IT equipment can operate within a facility. (These should also be included in the USSOs.)

d. Information on the appropriate methods for installing the equipment.

e. Details of the equipment inspection requirements and schedules as agreed with the appropriate authority.

Transmission Security

28. This sub-section is to provide details of, or make reference to, the following aspects, where appropriate, of transmission security:

a. A clear statement of who is responsible for implementing and controlling procedures for transmission security.

b. Procedures associated with the appropriate protection of authorized systems communications from analysis of the unencrypted sections of such communications.

c. Procedures for reducing the information content of the unprotected sections of communications.

d. Operational procedures for systems which provide traffic flow security.

Configuration Management

29. Configuration management of an IT system or network consists of identifying, controlling, accounting for, disseminating, and auditing all changes made during the design, development, operation, maintenance, and enhancement stages. It is to be noted that system encompasses both the Trusted Computing Base (TCB), where present, and any additional operating and application aspects in particular relating to the security-relevant features of hardware, firmware, and software.

30. This section is to provide details of, or make reference to, the following features of a configuration management plan where these relate to security aspects of hardware, firmware, and software:

a. Personnel responsibilities for the control and organization of configuration updates.

b. The documentation describing the configuration baseline of the IT system.

c. The controls applicable to changes in specification and design documentation.

d. The controls applicable to changes in implementation documentation.

e. The controls applicable to changes in source code, the running version of the object code, test features, and test documentation.

f. The controls applicable to providing assurance that the current version of the system maps consistently with the documentation and associated code.

g. The controls applicable for the generation of a new version of the system including utilities and software packages.

h. The controls applicable to the re-generation of the operating system software, including utilities and software packages, at irregular intervals from the master versions prior to any authorized modifications being made.

i. The controls applicable to the comparison of a newly generated system, including utilities and software packages, with the previous version in order to ascertain that only the intended changes have been made.

j. The controls (technical, physical, and procedural) applicable to the protection, from unauthorized modification or destruction, of the master copy or copies of all material used to generate the system, including utilities and software packages.

k. System hardware, firmware, and software configuration modification request procedures.

l. Specific modification request procedures for the hardware configuration, or the system-related environment, where there is a need to comply with a TEMPEST standard; and specific post-modification implementation auditing.

m. Post-implementation procedures for amending configuration change documentation.

Annex - General Security Guidance To Users

31. An annex is to repeat in summary form the main user-originated procedures appearing in earlier sections. This could be utilized as a stand-alone document in the user environment. Some of the aspects which are to be covered include the following:

a. How to gain authorization to use the IT system or network.

b. Password, users identification and access control responsibilities.

c. System specific procedures for handling and storage of protectively marked documents.

d. What records are to be kept.

e. How to report problems, malfunctions, and suspected security breaches.

f. Users' general security responsibilities.

g. Downgrade and sanitization procedures.

Conclusion

32. SyOPs form an essential component of how security is applied to IT systems and networks and address all aspects of security, not just hardware and software. SyOPs should be formulated with great care and attention to detail. Users should be made fully conversant with their relevant aspects of the SyOPs and understand their implications in order that they may play their full part in the achievement of overall security and should sign to signify that they have read them.

ANNEX G TO

CHAPTER 3

THE PROJECT REGISTRATION FORM (PRF)

PROJECT REGISTRATION FORM (PRF)	
Project Name	
Reference Number	
PRF Version	
PRF Date	
PROJECT MANAGEMENT AUTHORITY (PMA) DETAILS	
PMA Title	
PMA Contact Name	
PMA Contact Phone	
PMA Contact Email	
Will This Project Have a SAC ?	Yes / No
SYSTEM PROFILE	
Maximum Protective Marking	
Criticality Level	CL
Number Of Users	
Operating Mode	
External Connections (List)	
ACCREDITATION REQUIREMENT	
Sectors Affected	
Links To Allies or OGD (List)	
TIMESCALES	
Tender Issue	
Contractor Selection	
Initial Operating Capability (IOC)	
Full Operating Capability (FOC)	
Security Policy Documentation (SPD) Type - ADS or Legacy	
Security Working Group (SWG) Frequency	per year
Requested document turn-round cycle	days
REGISTRATION CONFIRMATION	
Estimated Annual Workload	days
Allocated Accreditor(s)	
Signature of Lead Accreditor	
Date	

This page intentionally left blank.

ANNEX H TO

CHAPTER 3

INFOSEC SCOPING APPRAISAL (ISA) TEMPLATE

INFOSEC SCOPING APPRAISAL FOR 'PROJECT NAME'

Document reference, Date

REFERENCES

BASIC INFORMATION AND SECURITY SCOPE SUMMARY

Key Security Characteristics	Maximum Protective Marking	Minimum Clearance	Criticality Level	Authorisation		
Business				Yes	No	N/A
Infrastructure				Yes	No	N/A
Connections				Yes	No	N/A
Security Risk Category						
Project reference						
Accreditor(s)						
Next Project Milestone & Date						
Document Status						
Approved by						
Prepared by						

1. Give a paragraph describing the objective of the project and references to further information.

Business And Information Exchange Requirements

2. Give a description of the security aspects of the business requirements, identifying all people involved in the business process. This should cover all areas of business, including the business done with any existing or planned interconnected systems. Protective Markings, Criticality Levels, caveats, codewords, nationality, indoctrination and numbers should be given, or an indication of the expected bounds.

Infrastructure And Architectural Constraints

3. Give a description of the security relevant infrastructure and architecture constraints, identifying all people with access to shared infrastructure and any onward connections. Protective Markings, Criticality Levels, caveats, codewords, nationality, indoctrination and numbers should be given, or an indication of the expected bounds.

Outline Operational Security Management Plan (OSMP)

Roles and Responsibilities

4. Identify any factors affecting security management for the in-service system, including any significant skills or training requirements that can reasonably be envisaged at this stage.

Physical, Radiation and Communications Security

5. Identify any factors affecting the satisfactory provision of security in the expected locations of equipment and personnel. Identify the security characteristics of any people with unescorted physical access to equipment.

Security Operating Procedures (SyOPs)

6. Identify the different kinds of SyOPs that will be produced and the groups of people they will apply to.

Security Risk Categorisation

7. Explain the factors in the choice of Security Risk Category for the project.

Appraisal

8. Give the results of an appraisal of the key security risks to the operational system arising from the overall requirements, making clear any assumptions. Security concerns that give rise to project risk should be identified. Describe why other security concerns are not considered to be a risk to the project.

Outline Infosec Management Plan (Imp)

Roles and Responsibilities

9. Identify how any requirement for a Security Working Group is to be addressed and/or responsibility for the full IMP, if required.

Project Context and External Dependencies

10. Identify any significant security-relevant links or dependencies with other projects, organisation or events.

Accreditation Evidence Requirements

11. Give an outline of how the accreditation of the system will be managed, for example requirements for interim accreditation, arising from incremental acquisition or rollout, and the information it is intended to supply as evidence to support each accreditation decision. Give an indication of the expected timescales.

Project Milestones

12. Identify any agreements with the accreditor that are anticipated for key project milestones, such as Initial Gate, Main Gate, ITT for a development contract, user trials and evaluation or Health Check activities.

Project Security

13. Identify any factors affecting project security, for example the need for cleared development staff or a secure development area.

Project Risk Management Summary

14. Use the table below to describe the security-related risks to the project identified by the scoping appraisal and how these risks are to be managed, for example an area requiring further study as part of the Infosec Risk Management Appraisal process. This section may be presented as an annex to the ISA for ease of use.

Id.	Description	Strategy
1		
2		

This page intentionally left blank.

ANNEX I TO

CHAPTER 3

INFOSEC MANAGEMENT PLAN (IMP) TEMPLATE

Template

1. An Infosec Management Plan (IMP) is one of the concepts being developed under the Domain Approach, and a formal template was not available at the time of publication. Instead, the following general guidance should be taken in account when producing an IMP. In due course, this Annex will contain a template, supported by guidance in Defence Information Assurance Notice No 7 'Security policy Documentation'.

General Guidance

2. An Infosec Management Plan (IMP) is concerned with the accreditation process for a project, or group of related projects. It does not provide evidence in support of accreditation.

3. An IMP is the means whereby agreement is reached with the accreditor on what is necessary in this particular project(s) for the Accreditation Evidence Statement (AES) for each accreditation decision and what additional agreements with the accreditor are planed during the project. An IMP will contain much of the information that would normally be provided in Chapter 1 (Introduction) of a Memo 5 SSP. Note that an IMP may also be used to describe generic requirements for several projects, as a replacement for a Memo 5 Community Security Policy (CSP).

4. The level of detail appropriate for an IMP will depend upon the complexity of the project(s) and Infosec detail in other project documentation and plans. In some cases, an IMP may be a simple extraction of relevant information from other documentation that is presented to and endorsed by the accreditor. In other cases, the IMP may be component of the general project documentation.

5. An IMP may contain, or refer to, information about the:

a. Project Infosec roles and responsibilities, including

i. Procedures, mechanisms and responsibilities for updating the plan;

ii. Security Working Group and/ or other security advisors to the project;

iii. Links and dependencies with other IMPs, projects, programmes, organisations or events.

b. A summary of the security-related project risks;

c. Required contents of the Accreditation Evidence Statement (AES) for each planned accreditation decision;

d. Planned Infosec activities (covering timescales and relationship to other project activities such as budgetary approvals, contract let and the non-security specific documentation):

i. Definition the Target of Accreditation (or redefining an existing one);

ii. Security documents to be produced during the project, identifying which will require the accreditor's endorsement;

iii. Activities required by the AES, including the production of security documents;

iv. Security-related design work, pilots, trials, etc.

6. Not all information need necessarily be known at each stage in the project. Furthermore, as the IMP is a management tool, not all the information need necessarily be formally endorsed by the accreditor. However, the accreditor may be able to provide advice, based on experience and knowledge of projects.

APPENDIX 1 TO

ANNEX I TO

CHAPTER 3

ACCREDITATION EVIDENCE STATEMENT TEMPLATE

1. It is the responsibility of the either the System Operating Authority (SOA) and/or Equipment Support Manager (ESM) to ensure that their systems are approved by all necessary bodies for operation, and therefore it is the responsibility of the SOA/ESM to request Accreditation.

2. For those systems being procured under Vote 3 procedures, the Project Management Authority (PMA) is responsible for seeking all approvals until the point that the system is Technically Transferred (TT) to the OA or ESM.

3. Under the review of Security Policy Documentation structures for MOD, it has been recommended that a "Portfolio" approach be adopted, rather than the monolithic SSP-driven structure previously used. Two of the elements of such Portfolio are the Infosec Management Plan (IMP) and the Operational Security Management Plan (OSMP). The IMP is to be produced as soon as practicable after Inception and defines the Security Relevant activities during a system LifeCycle as the milestones towards achieving Accreditation. The OSMP will define the milestones in support of Compliance during Operation.

4. The project-specific contents of the Accreditation Evidence Statement (AES) will summarise the status of progress towards milestones as an Annex to the IMP. Once accreditation has been achieved the AES will be attached to the Accreditation Certificate.

5. An AES would normally be produced in preparation in advance of each of the critical activities for a project by the Security Assurance Co-ordinator (SAC), to be used initially by the PMA/ESM/OA to gauge progress, and then when an Accreditation or Compliance milestone is reached to submit the request for Security staff action in a manner which neatly summarises the status of the project in security terms.

6. For projects that are not, or have not as yet, adopted the portfolio approach to security an AES should still be produced as a standalone document unless or until an

IMP or OSMP is available.

7. An example of a template from which a project-specific AES can be produced is attached, and it is stressed this is a very generic template, which will need customisation to meet special circumstances for each project, It should, however, be enough to ensure that at least the major generic concerns are addressed.

8. The structure of the AES has been designed to allow as much essential information as possible to be summarised on ideally one side of A4. The header block is largely self-explanatory, but the main body of the table need some clarification :

Column Title	Description	Usage
Components or Activities	Specific Security-Relevant activity	Either non-technical (Organisation & Management, Physical, Media, Personnel, Procedural) or Technical (the 3 sub-disciplines of Infosec – Comsec, Compusec and Radsec)
Target Date		This is used to show targets, for instance the ETR should be produced 9 weeks before any request for full Accreditation to allow for the ITSEC CB staffing times for a Certificate
Status (R/A/G)	A “traffic-light” to show current status, which can be either Red (R), Amber (A), or Green (G)	RED : No progress made, or serious problem encountered AMBER: Progress being made towards target for stage of OSMP, but either not completed or minor problem encountered GREEN: Achieved target in OSMP
Notes	Explanations or Expansions	GREEN : Typically document references to the successful state of the activity AMBER : Details of shortfall and planned resolution RED : Details of problem and impact statement

Project Name:	<Name>	**Prepared by and Date:**	<CWG> / <IPT>
Unclassified description	<Details>		
Certification Type:	<ITSHC> / <ITSEC> / <CC>	**Criticality Level:**	<n>
Accreditor(s):			

Accreditation Documentation Components	**Target Date**	**Status R/A/G**	**Notes**
Security Requirements Statement			
Security Risk Assessment			
Security Aspects of the Design			
Operational Security Management Plan			
OSMP Annex - IRP			
OSMP Annex - ECP			
OSMP Annex - ICSyI			
OSMP Annex - TOMSyI			
OSMP Annex - USyI / SSyI			
Codes of Connection			
Evaluation Security Target			Derive from SAD.
Evaluation Technical Report			Produced by CLEF.
Evaluation Certification Report			Produced by CB.
System Configuration Model			
Required Accreditation Activities	**Target Date**	**Status R/A/G**	**Notes**
Short Term Programme Provision			Evidence necessary resources available.
GFE ordered			<Grade>
Key Variables allocated			<Grade>
GSE/LSE Inspection			<Frequency and coverage from Ch 12>
ESE Inspection			<Frequency and coverage from Ch 12>
Vulnerability Analysis (Health Check)			<Frequency and coverage from Ch 12>
COMSEC Routine Inspection			<Frequency and coverage from Ch 12>
TEMPEST Visual Inspection			<Frequency and coverage from Ch 12>
IDA/CIDA Conformance check			<Frequency and coverage from Ch 12>
RadSec On-site Test			<Frequency and coverage from Ch 12>

This page intentionally left blank.

ANNEX J TO

CHAPTER 3

INFOSEC RISK MANAGEMENT APPRAISAL (IRMA) TEMPLATE

Template

1. An Infosec Risk Management Appraisal (IRMA) is one of the concepts being developed under the Domain Approach, and a formal template was not available at the time of publication. Instead, the following general guidance should be taken in account. In due course, this Annex will contain a template, supported by guidance in Defence Information Assurance Notice No 7 ‘Security policy Documentation'.

General Guidance

2. Not all projects will need to conduct an Infosec Risk Management Appraisal. Whether one is required it is expected to have been be agreed with the accreditor through the Infosec Management Plan (IMP).

3. An IRMA is equivalent to some of the drafts and/or early versions of a Memo 5 System Security Policy (SSP) that were produced in the early stages of projects for purposes other than accreditation evidence.

4. The objectives of the appraisal are:

a. Propose options for the Target(s) of Accreditation and consider them in sufficient depth to be able to assess and compare the user and management implications, security implications, project risks and costs of each option;

b. Select an option;

c. Agree a plan between the project team, user community and accreditor(s) that is likely to provide an accreditable, technically feasible and operationally effective system;

d. Record the rationale for the above decision, to facilitate impact assessment for future change proposals;

e. Identify the key risks to the project arising from the agreed plan and how these will be managed;

f. Ensure that the resources likely to be required to develop, document and maintain security for the chosen option have been identified by the project.

5. An IRMA document should contain, for each option that was considered during the appraisal:

a. A description of the security aspects of the business requirements' with no significant uncertainty remaining. This should cover all areas of business, including the Information Exchange Requirements for the business done with any existing or planned interconnected systems;

b. A description of the security relevant infrastructure constraints, with no significant uncertainty remaining. This should cover all the infrastructure required, and take account of all other purposes for which the infrastructure will be used, including connections to other infrastructure components;

c. A discussion of the impact of the security requirements and architecture in terms of how the users and administrators of the final system are expected to conduct their business;

d. An appraisal of the likely security risks in terms of compromise of confidentiality, integrity or availability and the evaluation assurance levels that are likely to be required of the security barriers (based on an Infosec Standard No 1 risk assessment);

e. A discussion of the security-related project risks, including any departures required from high level policy or existing agreements, such as Codes of Connection (CoCos) or Interconnection Security Measures Statements (ISMS);

f. Any links and dependencies with other projects or organisations and the relationship to high level requirements, such as those in the organisation's Business Continuity Plan;

g. The key assumptions and decisions made and the reasons for acceptance or rejection;

6. An IRMA should also identify how the risks arising from the chosen option will be managed.

7. Note that the business requirements need not be the same for each option, but may be modified to compromise on possible a workable secure solution. For example,

a business aspiration for web sharing may be modified to email to accommodate the need for a wide disparity between the clearances of people who aspire to share the information. Alternatively, the business process could be modified to exclude those with insufficient clearance from the web. The IRMA discusses the impact of such compromises on the business aspirations, for example the business impact of email rather than web or of a smaller group sharing the web.

8. An IRMA should always be agreed between the project, user community and accreditor. Responsibility for production of an IRMA would rest with the project, although it may be produced in conjunction with industry consultants and security advisors.

This page intentionally left blank.

ANNEX K TO

CHAPTER 3

SECURITY RISK ASSESSMENT (SRA) TEMPLATE

Template

1. A Security Risk Assessment (SRA) is one of the concepts being developed under the Domain Approach, and a formal template was not available at the time of publication. Instead, the following general guidance should be taken in account. In due course, this Annex will contain a template, supported by guidance in Defence Information Assurance Notice No 7 'Security policy Documentation'.

General Guidance

2. A Security Risk Assessment (SRA) is the document that justifies the security requirements placed on the Target of Accreditation. It is largely equivalent to Chapter 3 (Security Requirements) of a Memo 5 SSP.

3. The required contents of the SRA should be agreed with the accreditor as part of the Infosec Management Plan (IMP). A SRA may contain:

a. Threats, including environmental threats if applicable;

b. An explicit list of potential attackers;

c. An Asset Register assigning values and ownership;

d. Paths that could be used to compromise assets;

e. A Vulnerability Assessment, supported by completed worksheets relating to the requirements for security barriers (based on a HMG IS1 risk assessment as amplified by Annex B to Chapter 6), and/or reference to CRAMM risk assessment, if applicable;

f. A Risk Register identifying all security risks and how they are to be disposed. This will identify those:

i. risks that will be eliminated or managed within the Target of Accreditation;

ii. risks that are to be accepted;

iii. risks that are to be transferred to other agencies.

ANNEX L TO

CHAPTER 3

SECURITY REQUIREMENT STATEMENT (SRS) TEMPLATE

Template

1. A Security Requirements Statement (SRS) is one of the concepts being developed under the Domain Approach, and a formal template was not available at the time of publication. Instead, the following general guidance should be taken in account when producing a SRS. In due course, this Annex will contain a template, supported by guidance in Defence Information Assurance Notice No 7 'Security policy Documentation'.

General Guidance

2. A SRS defines the detailed security requirements for a specific Target of Accreditation against which the effectiveness of an implementation, or proposed implementation, can be assessed. An early version may also be used to support the ITT for a development contract. A SRS is equivalent to Chapter 2 (System Description) and some parts of Chapter 5 (Security Measures) of a Memo 5 SSP.

3. The required contents of the SRS may be agreed with the accreditor as part of the Infosec Management Plan (IMP). It is suggested that an SRS should contain the:

a. Maximum permissible connectivity of people and data for the Target of Accreditation in terms of the Protective Markings, caveats, and codewords of the business it does and the clearances, nationalities and indoctrination of the people who conduct that business.

i. The description will identify all the business data that requires protection and everyone who is involved in that business;

ii. This description must include all interconnected systems and the nature of the permitted connections. Hence it is a description of the total information process from a security viewpoint, including the Information Exchange Requirements.

iii. This description must have been agreed as workable with the user community;

b. Required security functions of the Target of Accreditation;

c. Other technical security-related requirements, such as architectural constraints, identifying all the people with potential electronic access, including those who are not part of the business process, such as subscribers to shared infrastructure;

d. Non-technical security requirements, such as physical and security management requirements, identifying everyone with potential physical access to the Target of Accreditation;

e. Details of which aspects of the above (a-d) are outside the scope of this Target of Accreditation and any security relevant assumptions that have been made about them;

f. Evaluation assurance levels, or other compliance testing activities, such as a Health Check, that are required.

ANNEX M TO

CHAPTER 3

SECURITY ASPECTS OF DESIGN (SAD) TEMPLATE

Template

1. The Security Aspects of the Design (SAD) document is one of the concepts being developed under the Domain Approach, and a formal template was not available at the time of publication. Instead, the following general guidance should be taken in account when producing a SAD. In due course, this Annex will contain a template, supported by guidance in Defence Information Assurance Notice No 7 'Security Policy Documentation'.

General Guidance

2. A SAD describes how the design and implementation of the system meets the requirements defined in the Security Requirements Statement (SRS). The SAD is also a key document with respect to risk traceability and can be used to ensure that proposed changes to the Target of Accreditation remain secure, as it links the implementation, SyOPs, Interconnection Security Measures Statements (ISMS), etc., to the Security Requirements Statement (SRS), and hence to the risk assessment in the SRA.

3. A SAD is equivalent to the system configuration in Chapter 2 (System Description), Chapter 4 (Security Domains) and some parts of Chapter 5 (Definition of Security Measures) of a Memo 5 SSP.

4. The required contents of a SAD, and any outline to be produced by the bidders for a development contract, should be agreed with the accreditor as part of the Infosec Management Plan. It is suggested that a SAD should contain:

a. Detailed description of the logical and physical aspects of the security design and implementation and the claimed assurance where applicable. Reference should be made to information supporting the claimed assurance, such as certification reports;

b. A description of the supporting non-technical aspects of the implementation, such as security management and physical aspects, including rationale and how they relate to the technical design, with reference to the detailed documents, such as SyOPs;

c. The assumptions that have been made about security that is outside the scope of the Target of Accreditation, and references to any relevant documents such as Service Level Agreements, Codes of Connection, Site Security Plans or Business Continuity Plans;

d. An explanation of how the requirements in the SRS have been met.

ANNEX N TO

CHAPTER 3

SYSTEM CONFIGURATION MODEL

1. The following represents a high level summary of the types of information that should be contained in a System Configuration Model (SCM).

2. It does not presume any particular methodology for maintaining this information, with examples currently in use being:

a. A text file places in %systemroot%\Profiles\AllUsers\Desktop on standalone WinNT systems to allow easy updating of changes made when in use by a number of different users from a pool ;

b. A loose leaf binder for small LANs ;

c. A relational database used for Asset Management and Installation Design control.

3. The major headings, which should be tracked, are as follows:

a. Management Responsibilities, including names, posts, and contact details ;

b. Hardware Details, including types, quantity and serial numbers, location, upgrades, references to Installation Design drawings ;

c. Software Details, including version details, licence numbers, and patch levels. Where manufacturer recommended patches have not been applied, the reason why should be recorded ;

d. System options, such as BIOS settings and hard disk partition formats;

e. User Details, including UserID, dates of activation, and level of privileges assigned.

This page is intentionally left blank

ANNEX O TO

CHAPTER 3

CODE OF CONNECTION (COCO) TEMPLATE

This generic template must be tailored so that it specifies conditions applicable to the assumptions of the project's risk assessment and the services being provided.

CODE OF CONNECTION FOR <NAME>

Reference, date

Purpose

1. This Code Of Connection (CoCo) defines the acceptable parameters for a system to connect to <name> such that the <name> risk assessment assumptions remain valid.

Authority

2. This CoCo has been authorised by the following signatories:

<name> accreditors	Signature	
	Post	
	Date	
	Signature	
	Post	
	Date	
<name> System Operating Authority (SOA)	Signature	
	Post	
	Date	

References

A. Relevant documentation for <name>, reference, date

Conformity

3. In order to connect to <name>, systems must provide evidence to the <name> System Operating Authority (SOA) that they meet an acceptable security standard. This shall be provided in the form of a Statement of Connection Conformity (SOCC) to the following conditions.

Condition	Specification
CoCo-1	A Connected System must be accredited as meeting national and departmental minimum standards, in accordance with JSP440.
CoCo-2	The minimum standards applicable to a Connected System shall be the greater of those required for the maximum security markings of data handled by the Connected System and <name>.
CoCo-3	The impact of all proposed changes to a Connected System shall be assessed for their impact on <name>.
CoCo-4	All existing and planned direct and indirect onward connections from a Connected System shall be brought to the attention of the <name> SOA prior to connection to <name>, and explicitly identified in the SOCC.
CoCo-5	The minimum clearance on a Connected System shall be <clearance>.
CoCo-6	No data Protectively Marked above <PM> shall be exchanged with or over <name>.
CoCo-7	All points of connection to <name> shall be within <geographical area>.
CoCo-8	Data may only be exchanged with or over <name> using the permitted types of business connection defined in the <name> accreditation documentation, Ref. A.
CoCo-9	Data exchanged with or over <name> must comply with the constraints on communications protocols defined in the <name> accreditation documentation, Ref. A.
CoCo-n	*Add, delete or amend as required*

Valid assumptions

4. A Connected System may make the following assumptions about the security provided by <name>:

<insert list>. *The list of assumptions about security must correspond to the functional services offered to a Connected System.*

Administration

5. Systems must complete and supply a signed copy of the SOCC given at Appendix 1 to the <name> System Operating Authority (SOA) prior to connection.

6. Systems that have a SOCC authorised by their accreditors are permitted to connect to <name> without recourse to the <name> accreditors.

7. Exceptionally, systems without such a statement may be given specific approval by the <name> system accreditors.

8. Any re-accreditation of a Connected System requires the SOCC to be re-authorised.

Appendix 1 to the <name> CoCo:

Statement of Connection Conformity of <connected system name> to the <name> Code of Connection

A. Operational Security Management Plan for <connected system name>, reference, date
B. Code of Connection for <name>, reference, date

Additional connections

<connected system name> is has direct connections to <insert list>.

<connected system name> is indirectly connected to <insert list>.

Authorisation

On the basis of the information made available to them, and to the best of their knowledge, the undersigned agree that <connected system name>, as defined by Ref. A, conforms to the requirements of Ref. B.

Any re-accreditation of <connected system name> invalidates this statement.

Signature:
Post:
Name:
Date:

Signature:
Post:
Name:
Date:

This page intentionally left blank.

ANNEX P TO

CHAPTER 3

INTERCONNECTION SECURITY MEASURES STATEMENT

Introduction

1. An Interconnection Security Measures Statement (ISMS) is equivalent to a short form Memo 5 SISP. An ISMS should contain the following as set out in the template below:

INTERCONNECTION SECURITY MEASURES STATEMENT

Between

(SYSTEM NAME) and (SYSTEM NAME)

This document defines the Interconnection Security Measures Statement (ISMS) for the connection called [*name of link (if applicable)*] between [*first system name*] located in [*location of system*] and [*second system name*] located in [*location of system*]. The document is subject to annual review and has been authorised by the following signatories:

(System Name)	(System Name)
……	…….
(name)	(name)
(title)	(title)
System Operating Authority	System Operating Authority
Date: ……..	Date: ……..
…….	…….
(name)	(name)
(title)	(title)
System Accreditor	System Accreditor
Date: ……..	Date: ……..

References:

[…] of […] SPD for [*name of first system*]
[…] of […] SyOPs for [*name of first system*]
[…] of […] SPD for [*name of second system*]
[…] of […] SyOPs for [*name of second system*]

This ISMS covers the link, called [*name of link (if applicable)*], between [*name of first system*] located in [*location of system*] and [*name of second system*] located in [*location of system*]. The link enables the controlled transfer of [*data files / Electronic Mail* …] between the two systems.

[*First System Name*] has been granted [Interim / Full] Accreditation and is permitted to handle data protectively marked up to [RESTRICTED / CONFIDENTIAL / SECRET / TOP SECRET]. It also has approval to handle the following: - [*COMINT / UK EYES / VRK* …].

The lowest clearance of any user of [*first system name*] is [BC / SC / DV]. [*Any other significant aspects of clearance, e.g. all users have a STRAP briefing, to be included*].

[*Second System Name*] has been granted [Interim / Full] Accreditation and is permitted to handle data protectively marked up to [RESTRICTED / CONFIDENTIAL / SECRET / TOP SECRET]. It also has approval to handle the following: - [*COMINT / UK EYES / VRK* …].

The lowest clearance of any user of [*second system name*] is [BC / SC / DV]. [*Any other significant aspects of clearance, e.g. all users have a STRAP briefing, to be included*].

[…] information **shall not** be transferred between the systems [*via E-mail* …].

[…] data may only be transferred using [*special software / procedures* …] and subject to the formal agreement [Reference …].

[*First System Name*] operated in [DEDICATED / SYSTEM HIGH / COMPARTMENTED / MULTI-LEVEL SECURE] mode of operation.

[*Second System Name*] operated in [DEDICATED / SYSTEM HIGH / COMPARTMENTED / MULTI-LEVEL SECURE] mode of operation.

No additional category of material may be put onto either system, nor may the secure mode of operation be changed, without prior approval of the appropriate security authorities.

Each System Operating Authority must inform the other System Operating Authority of any changes that may have an impact on security, especially changes to connectivity. This document is be reviewed annually on [*review date*] by signatories, or their successors, to confirm that the above conditions still apply.

ANNEX Q TO

CHAPTER 3

OPERATIONAL SECURITY MANAGEMENT PLAN

Template

1. An Operational Security Management Plan (OSMP) is one of the concepts being developed under the Domain Approach, and a formal template was not available at the time of publication. Instead, the following general guidance should be taken in account when producing an OSMP. In due course, this Annex will contain a template, supported by guidance in Defence Information Assurance Notice No 7 'Security Policy Documentation'.

Introduction

2. An Operational Security Management Plan (OSMP) is equivalent to Chapter 6 (Administration of Security) of a Memo 5 System Security Policy (SSP) and the SyOPs. The required contents and structure of the OSMP should be agreed with the accreditor as part of the Infosec Management Plan. In addition to the components defined in Chapter 3, an OSMP may contain the:

a. SyOPs covering particular configurations or deployment constraints;

b. Operational roles and responsibilities for security management, including the security management structure;

c. Roles and responsibilities of the Security Working Group, and/or other advisors to the operational security managers;

d. Re-accreditation conditions, covering both changes to the configuration and the impact of external change;

e. Regular security inspection activities.

Security Operating Procedures (SyOPs)

3. Procedural measures are a prerequisite foundation for security, and where the appropriate foundation has not been laid then it will be almost impossible to implement a secure system.

4. All systems that process official information are to be operated in accordance with relevant SyOPs. SyOPs are to be promulgated to all relevant staff and incorporated within standing security instructions/orders issued by Commanding Officers/Heads of Establishment/Directors or Heads of Division as appropriate. All significant amendments to the SyOPs are to be approved by the Accreditor.

5. Users should be required to sign to confirm that they have sighted and understood SyOPs at commencement of access to any CIS, and thereafter at a frequency to be agreed with the Accreditor.

6. The single set of SyOPs that are utilised for standalone computers or small networks will not be adequate for more complex systems, as these will require considerably more attention to the responsibilities of the staff actually running the IT system.

7. The primary purpose of SyOPs is to clearly communicate the procedures that are required to enforce security to the people who are responsible for its enforcement. Therefore, although it is important that each procedure is traceable back to the requirements, the rationale should be included in other Security Policy Documentation, rather than in the user and administrative documentation. SyOPs should be easily accessible, for example on-line and/or included with the general operating instructions. Ideally, User and/or Subscriber Security Instructions (USyI), should be as simple a possible, since a single, UNCLASSIFIED side of paper that can be left by the system terminal is much more likely to be followed than a large document that has to be secured due to its own Protective Marking.

8. SyOPs should:

a. Clearly indicate the procedures people should follow, for example in a check-list style wherever practical;

b. Cover all aspects of the non-technical security measures, including physical and procedural measures;

c. Clearly indicate to people how to use the technical security measures;

d. Clearly indicate their authority and the consequences of failure to comply;

e. Clearly indicate the form of compromise that may result as a consequence of not following the procedures;

f. Clearly indicate suspicious activity that should be reported, covering both technical attacks, such as unexpected dialogue boxes, and non-technical attacks, such as social engineering;

g. Enable users to give feedback on the operational effectiveness of the SyOPs, submit change proposals or be involved in reviews;

h. Be testable as part of an inspection or audit.

This page intentionally left blank.

APPENDIX 1 TO

ANNEX Q TO

CHAPTER 3

INCIDENT RESPONSE PLAN TEMPLATE

Introduction

1. Where an IT system, or the information contained on it, is vital to role or mission, there is a need for units and establishments to address the procedures to be carried out in the event that incidents occur. These procedures should be formulated in Incident Response Plans (IRP).

2. Incident Response Plans should be part of the Operational Security Management Plan (OSMP) and reference in the SyOPs. They should be agreed with the system Accreditor. The plans should be relevant to the system, comprehensive (depending on the importance of the system to the unit/establishment), and exercised regularly.

IRP Template

3. An IRP is one of the concepts being developed under the Domain Approach, and a formal template was not available at the time of publication. Instead, the following general guidance should be taken in account when producing an IRP. In due course, this Annex will contain a template, supported by guidance in Defence Information Assurance Notice No 7 'Security Policy Documentation'

Background

4. Terminology :

a. **Incident** – Any Event affecting a CIS with security relevance ;

b. **Intrusion** – Any set of actions that attempt to compromise the Integrity, Confidentiality or Availability of a Security Barrier ;

c. **Attack** – Any Incident or Intrusion with Intent.

5. The following matters serve as indicative list of the issues that may be considered as CIS Security Incidents :

a. Damage / disaster ;

b. Theft ;

c. Physical infiltration ;

d. Hacking :

(i) Internal ;

(ii) External “hobby hackers” ;

(iii) Electronic attack “an attempt to gain unauthorised access to an IT system over an electronic network, in order to disrupt its operation or to gain access to information for intelligence purposes” ;

e. Misuse of resources;

f. Malicious software:

(i) Virus;

(ii) Worm;

(iii) Trojan;

g. Failure (hardware or software);

h. Personnel error;

i. Personnel shortage.

Monitoring And Detection

6. Who ?

7. How ?

8. Receipt and Handling of Alerts

9. Recording of Incidents

10. Preservation of Evidence

Triage

11. The term "Triage" is used to describe the assessment of severity of any incident, and deciding the mature of follow up action required.

12. Upon detection of an Incidents, apply the following 5 stage analysis to decide upon action required :

Incident Type	Response Type	Response Time	Coordination By
Offensive IW	Military	Immediate	PJHQ
Serious Breach	Security	Immediate	ISyDO
Serious Crime	Police	Immediate	MDP CIR
Technical Infosec	Technical	Dependent on Criticality Level (CL)	
Other Incidents	Unit	Dependent on Criticality Level (CL)	

13. Where the response required is dependent on Criticality Level (CL) of the CIS affected, the following metric should be applied

Criticality Level	Response Time	Coordination By
CL1	Immediate	ISyDO
CL2	Within 8 hours	Sector Duty Officer
CL3	Within 1 working day	PSyAs
CL4	To Unit Priorities	Unit Security Staffs

Escalation Routes

14. During working hours, incidents should normally be progressed through the Security Chain of Command if applicable, but for times where it is unclear within which PSyA remit a matter lies, or for significant issues that occur outside core working hours, the MOD maintains an Information Security Duty Officer (ISyDO), which is a role fulfilled by members of D Def Sy staff.

15. The ISyDO is nominated to the Government CERT as the MOD's first point of contact for information security problems, and for OGDs reacting to electronic attack.

16. During core working hours, the ISyDO can be contacted via the D Def Sy Duty Line. The Ministry of Defence Police (MDP) Central Information Room (CIR) act as the initial point of contact for the ISyDO outside core working hours, and can be contacted as follows:

Telephone (MOD Network)	Wethersfield (WFD) Ext. 4444
Telephone (GTN)	3056-4444
Telephone (PSTN)	+44-1371-85-4444

Facsimile (MOD Network)	Wethersfield (WFD) Ext. 4030
Facsimile (GTN)	3056-4030
Facsimile (PSTN)	+44-1371-85-4030
Telex	98144MODPOL G
Signal Message Address	CCMDP WETHERSFIELD
Use SIC(s)	Y3B

Reporting

17. **It is required that all suspected, attempted, or actual incidents and weaknesses are to be reported to the relevant Security Authority(s), via the security chain of command if applicable.**

18. Internal reporting

19. External reporting

20. Where possible, such reports are to made by PRIORITY signal, or facsimile, in order not to delay a return to normal working whilst a security investigation takes place. A signal format is given at Annex A to Chapter 10. If in doubt, contact the security chain of command.

21. In all cases, a full UNIRAS report is to be made using form GS490 ("Report of IT Security Incident") or GS490A ("Report of IT System/Product Weakness"), marked according to the maximum protective marking of the data processed, minimum RESTRICTED (see Annex B).

22. The form is to be completed by the unit/establishment at the site of the incident and is to be sent to the relevant Security Authority, via the security chain of command. If in doubt as to which form to complete, contact the security chain of command or Security Authority. On no account is the vendor of a faulty product to be informed without first seeking the advice of the Security Authority.

Breaches

23. Certain categories of incident will where it is likely that a compromise of Protectively Marked Information require more in-depth investigation, and ESyOs/ITSOs should consult the PSyA or ISyDO direct for instances of :

a. Cases of serious, ongoing or unexplained breaches of security ;

b. Where a possible compromise of systems handling TOP SECRET, STRAP, or other Compartmented material is suspected or detected ;

c. All detected or suspected instances of "hacking", especially those from a source external to the MOD.

Disciplinary And Criminal Considerations

24. In addition to Information Security concerns, CIS Incidents may also involve disciplinary and criminal considerations, which unless a serious Breach of National Security is indicated, may take precedence over any Security investigation required. The following paragraphs provide guidance on handling of these types of incident, and in case of doubt the PSyA or ISyDO should be consulted before proceeding.

25. The Ministry of Defence Police has a special investigative capability for Computer-based evidence, who can be contact for advice :

Ministry of Defence Police Fraud Squad
Computer Examination Unit
MDP Wethersfield — Tel: 01371 85 4465/4466
Braintree, Essex, CM7 4AZ — Fax: 01371 854313

26. **Malicious Damage and Theft.** Deliberate damage to, and theft of, MOD CIS asserts is clear indication of a criminal act having occurred, and other than in cases where a serious breach of security has also occurred, the pursuit of such incidents should normally be through the Ministry of Defence Police (MDP) or, for cases solely involving Service Personnel, the appropriate Service Police.

27. **Physical infiltration.** The physical infiltration of a MOD site by unauthorised persons should be dealt with by either local security staffs or through the Ministry of Defence Police (MDP) or, for cases solely involving Service Personnel, the appropriate Service Police, as laid down in JSP440 Volume 1. Any collateral incidents (e.g. Theft) should, however, be assessed against the guidance in this Chapter.

28. **Electronic attack.** An “electronic attack”, sometimes referred to as a Computer Network Attack (CNA), is any set of actions by any entity (group or country) hostile to the UK that deliberately attempt to compromise the Integrity, Confidentiality or Availability of a Security Barrier. A hostile entity will normally be either a Terroist / Extremist organisation or the military or intelligence apparatus of a unfriendly power, and will thus normally require a national response.

29. **Misuse of resources.** Improper use of MOD CIS facilities comprises an ever widening range of activities and behaviour, contrary to Security Operating Procedures (SyOPs), sound practice, or commonsense. It can be as a result of a deliberate action, or of an unintentional action or failure to act, but for the purposes of this manual, CIS improper use is defined as the deliberate, inappropriate or illegal use of any part of the MoD’s IT facilities.

30. A general list of prohibited use of MOD CIS can be found at Annex E, with the most common incidents including the sending of offensive/abusive or excessive ("spam") e-mail; the use of e-mail or other facilities for private commercial purposes; the use of sexually explicit material as desktop `wallpaper'; the importation, distribution and use of unauthorised software (including graphics files, text files, computer games and many other variants); and accessing, without permission, of non work-related Internet sites, typically for Downloading or Forwarding of Indecent Material.

31. All staff are responsible for ensuring that both they, and their colleagues, use these facilities in an appropriate, lawful and effective manner. All staff have a responsibility to report to their line management any suspected cases of IT misuse which they encounter, irrespective of their personal views on the severity of the alleged offence, or whether or not they have been directly affected or offended by the activity in question. Someone receiving, for example, sexually explicit material via MoD IT facilities has a responsibility to report the matter, even if they do not personally take offence.

32. Line managers, in turn, must consider what, if any, action to take in accordance with the relevant disciplinary procedures set out in the MoD Personnel Manual and other Instructions. Disciplinary action may be taken against any member of staff who misuses MOD's IT facilities, or even attempts to do so. This may result in dismissal.

33. When undertaking evaluations prior to contacting MDP where cases of misuse are suspected, care should be taken not to take any action that might later prejudice a criminal investigation. Guidance on preservation of evidence is given at Annex D.

34. Before taking an action therefore, Security Staffs should contact either the designated Information System Misuse Officer (ISMO) within their PSyA, or, for urgent matters outside of core hours, the MOD Information Security Duty Officer (ISyDO), who will advise on appropriate action to be taken. Where criminal activity is suspected, the involvement of the Ministry of Defence Police (MDP) or, for cases solely involving Service Personnel, the appropriate Service Police, will normally be sought thereafter.

35. In the particular case of any case of Indecent or Obscene Material being found on systems, due to certain legal requirements it is stressed that all local investigations should be ceased until either a Police Officer ,or a PACE trained ISyDO / ISMO registered with the MDP, can be attend to assess whether the material discovered does indeed constitute "Indecent or Obscene" matter, and use an agreed severity categorisation to determine whether the matter should be progressed as Disciplinary, Security and/or Police matter.

36. It should be noted that the involvement of Police may have serious implications for business continuity where, for example, it is necessary to impound CIS equipment in order to carry out any investigations arising.

37. **Malicious software.** Although, by simple definition, an infestation by Malicious Software is *prima facie* evidence of a breach of the Computer Misuse Act (CMA), only in cases where the infestation appears to have been deliberately and specifically targeted at MOD will a Criminal Investigation, involving Service Police or MDP, be required.

System Weaknesses

38. IT systems often contain faults which come to light only after extensive use, or when unusual conditions enable them to be discovered. Occasionally, these faults are already known to the manufacturer or supplier; often, they are not.

39. In order that the appropriate security and/or technical authorities can react to make systems less flawed or susceptible to misuse, possible security weaknesses or faults, are to be reported. The importance of reporting these incidents cannot be over-emphasized. Even a problem discovered on an UNCLASSIFIED computer may have implications for a Protectively Marked system running on similar hardware or software, or using similar procedures. Moreover, systems may have an operational significance additional to the level of protection required by the data held. All such incidents are to be reported.

Hoaxes

40. The Internet is constantly being flooded with information about Malicious Software (e.g. computer viruses and Trojan Horses). However, interspersed among real Malicious Software warnings are hoaxes. Whilst these do not infect computer systems, they are still time consuming and costly to handle.

41. In particular, a number of issues are commonly raised about emails, and the following should therefore be noted :

a. Email messages, by themselves, cannot currently be directly invoked as computer viruses.

b. However, malicious code may be contained in Email file attachments, e.g. word processing files, and should therefore be treated accordingly.

c. Messages may also contain URLs or hypertext links that point to Web-sites with malicious code that can unwittingly be imported by the user.

42. All Malicious Software alerts confirmed as originating from UNIRAS may be regarded as Authoritative, and only MOD Security Authorities, CM(IS), or the Sector

DCIS staffs should normally be regarded as an Authoritative Instigators of Alerts to the MOD community.

43. A Defence Information Assurance Notice (DIAN) is issued by the Defence Infosec Working Group (DIWG) on a regular basis that list Hoaxes known to be circulating, and in the case of warning received from elsewhere this should be consulted as an initial reference, as in most cases it will indeed prove to be a Hoax.

44. Should the Hoax DIAN not reference the matter reported in the unconfirmed warning, for instance in the case of "new" Hoaxes, then the following list of Internet Uniform Resource Locators (URLs) are useful Open Source references on this topic, which are widely accepted as being Authoritative Public Domain Sources, and will normally be kept current with the newer Hoaxes :

http://ciac.llnl.gov/ciac/CIACHoaxes.html

http://www.datafellows.com/hoax.html

http://www.drsolomon.com/vircen/vanalyse/va005.html

http://kumite.com/myths

http://www.sophos.com/virusinfo/scares/

http://www.symantec.co.uk/avcenter/hoax.html

45. Where no such correlation is found, PSyA should then be consulted who will advise as to whether a UNIRAS Report to definitively establish the veracity of the alleged Alert is required.

Investigations

46. Investigations into minor breaches and compromises are normally performed on behalf of the Head of Establishment by local Security Staffs, and Major Investigations will be performed under the remit of a PSyA in the case of systems with Sole Accreditation, or an Accreditation Panel for Joint Accreditation.

47. Major investigations will normally carried use the specialist security staffs provided at Sector levels for the Inspection function, and may be augmented by additional staffs from other areas of MOD, Government, Police, or contract support personnel, where particular technical or investigative expertise is required.

48. Major Investigations are considered to be part of the security compliance checking activities, as they are normally instigated due to Incidents that have been a result of either a failure and/or breach of security policy. The result of Investigations can be used to reinforce the security posture of the affected system(s) in the future. The investigation report, using the same style of gradings for recommendations as for an

Inspection as laid down at Chapter 11 Annex H, is therefore supplied to the Accreditors evidence for the continuance of Accreditation.

49. In the event of a suspected attack on Defence IT systems by malicious software, the actions laid down at Chapter 10 Annex C must be taken.

Recovery

50. How ?

Closures

51. How ?

This page intentionally left blank.

APPENDIX 2 TO

ANNEX Q TO

CHAPTER 3

EMERGENCY AND CONTINGENCY PLANS TEMPLATE

Introduction

1. Where an IT system, or the information contained on it, is vital to role or mission, there is a need for units and establishments to address the procedures to be carried out in the event that the IT system becomes unserviceable and the data processed/stored is unavailable. These procedures should be formulated in emergency and contingency plans.

2. The full topic of Business Continuity Planning (BCP) is without the scope of JSP440, and units wanting further information should contact :

Name

Post

Telephone

3. The system Accreditor will however wish to see that at least the system specific elements of BCP have been addressed in the form of a Emergency and Contingency Plan, which will normally be provided as an Annex to the Security Management Plan (SMP). Security Operating Procedures (SyOPs) should also contain links to the ECP, normally within the Technical Operation and Maintenace Security Instructions (TOMSyI), but if relevant also within the User Security Instructions (USyI).

Situation

4. Emergency and contingency plans cover the following eventualities:

a. Loss of Computing Power/Capability. This could be through equipment failure or a disaster such as a fire or terrorist attack.

b. Loss of Programs or Data. A system failure such as a head crash or a virus attack could destroy or corrupt data.

c. Loss of Computing Personnel. This could be as a result of illness, a terrorist attack or a fire.

d. Unavailability of Computer Buildings or Facilities. This could be as a result of structural damage to the building or offices housing the system or to a planned or unplanned move.

Back-up Procedures

5. All units/establishments with IT systems are to have a regular programme of back-up of data stored on the system. The frequency of back-ups should be decided between the users and the ITSO and should be detailed in SyOPs. The provision of back-ups will negate the more serious effects of incidents which affect an IT system.

6. Back-ups should be afforded the same protection as the live data held on the system. Back-ups should be held separately from the live data and ideally in a different location to the system.

Content

7. Emergency and contingency plans are to encompass the following:

a. Standby Facilities. Standby facilities include the provision of back-up computers, computer components or the provision of back-up facilities, such as power supplies. Whatever is decided these facilities should be afforded the same protection as the live system and be commensurate with the mode of processing.

b. Files/Documents. Copies of files and documentation must be available at the standby site, if there is one, to enable computer operations to continue.

c. Standby Staff. Arrangements should be made for staff to undertake the activities of absent personnel. Additionally, arrangements will need to be made for staffing at standby sites.

d. Logistical and Administrative Support. Arrangements must be made for the transportation of back-ups to their secure storage, similarly for their return to the system when needed. Additionally there should be details of the movement of hardware, software, documentation, staff, etc, and for administrative support required at a standby site.

e. Evacuation/Destruction Plan. Arrangements should include details of the evacuation of the IT installation and/or the offices containing the IT system. These should address the requirements for different situations, e.g. fire and terrorist attacks. Additionally the requirements for the destruction of protectively marked material should be included, especially in an emergency.

f. Recovery. Detailed arrangements for the return of the system back to normal processing should be clearly defined. Where applicable this should also encompass the secure closure of any standby site.

Relevance

8. Emergency and contingency plans are to be relevant to the system they refer to.

9. In determining the pre-planning that will be required for an ECP, the following table should be used, based on the Criticality Level (CL) of the CIS in question. It should be noted that measures are additive, so that the requirement for CL1 includes all those specified for CL2-4.

System Criticality	**Objective**	**Countermeasures**
CL1	Provide sufficient countermeasures for additional protection against special risks or special threats (accidental or malicious)	Flexible Power backup Multiple, diverse routed communications links Redundant and diverse processing capacity
CL2		
CL3		Short term backup power Data backup with remote storage Fallback communications links Standby processing capacity
CL4	Provide general protection against normally forseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations)	Defined Contingency Plan Data backup with local storage, at frequency defined in SyOPs

10. The efficacy of an ECP can only be achieved if they are exercised regularly. These exercises should not be restricted to the same scenarios but to all scenarios identified in the threat to the system. A regular programme of exercises are to be established and practised. Lessons learnt are to be promulgated among the staff and SyOPs altered if required. Similarly the plans may need to be amended.

This page intentionally left blank.

ANNEX R TO

CHAPTER 3

GUIDELINES FOR THE PRODUCTION OF SYOPS FOR UNIX SYSTEMS

1. Introduction.

a. Aims of SyOPs.

List any systems that are networked and have their own System Operating Procedures.

2. Administration: Responsibility and Control.

a. General

(1) State name(s) of systems covered locations, person or post responsible for management.

(2) Define system posts and responsibilities.

(3) State the highest protective marking level on the system and mode of operation (eg System high).

(4) State the route for obtaining advice on security.

(5) Designating and reporting breaches.

(6) Distribution of SyOps.

(7) Change control procedure for SyOps.
(in annex to avoid having to re-approve the entire document)

b. Unix specifics.

(1) Reference a directory of authorised users produced from a password file.

(2) Document change control procedure.

Protection of the password file or directory.

(3) List UNIX sub-systems not allowed (eg EMAIL, XWINDOWS)

c. Engineering and other support staff.

How such staff are to produce a hard copy log.
Clearance level of Engineers.

3. Personnel Security

a. Introduction.

b. Security education requirements.

Training courses.
Maintain awareness.

c. List of users with routine access to the system equipment.

Annex so that the list can be changed without having to agree the whole document.

4. Physical Security

a. Introduction.

Note the risk of gaining 'root' privileges through access to system equipment and console.
Root, superuser or other system wide privileges (Annex)

b. Layout plan and equipment list.

c. "The two-persons present rule".

If it can be used, description of how.

d. Secure startup and shutdown procedures naming users responsible.

Disabling logins.
Hardware/software disabling of communications external to the area.

e. Control of access to area.

Intruder alarms and the response.
List of persons authorised to open the area.

f. Access controls for visitors and engineers.

Control of diagnostic equipment in and out.
Control of media brought in.
Control of documents and media leaving, including check of protective marking.
Supervision of engineers.

5. **Document Security**.

a. Introduction

Definition of document.

b. Identification of printed output.

Use of labelling software.

c. Control of printed batch job log files.

Delaying prints.

d. Control of magnetic media.

Labelling.
Access to media library.
Destruction procedure.
Logging use.
Policy on import of media (eg virus control)

e. Control of device files within /dev directory.

Mechanism for assigning tape drive to users.
Logging assignment of devices.
Control of mount of tape.

f. Control of documents produced from printers attached to terminals.

6. **Hardware Security**.

a. Introduction.

b. Hardware configuration management.

Change control.

(1) Physical re-configuration.

Preparation and purging
Disconnecting devices
Checking result.

(2) Software (logical) re-configuration.

c. Engineering and maintenance control.

(1) General.

Warning about contents of swapfiles etc.

(2) Hardware monitoring.

Security rules
Checking for protectively marked data on system.

(3) Hardware diagnostics.

Downgrading beforehand.

(4) Removal of failed hardware/media from the site.

Prior arrangement for maintenance
Disposal.

(5) System integrity checking.

Running HW diagnostics.

(6) System dumps.

d. TEMPEST protection. [BTR/01/3(91) & BID/01/200(3)]

Warning about requirements.

7. **Software Security**.

a. Introduction.

Note about degree of trust.

b. System re-configuration by software.

Disabling logins
Access to peripherals.

c. Hardware re-configuration during system startup.

Building Unix
Device drivers.

d. Purging memory.

Use of purge utilities.

e. Username/ password management.

Note about where responsibility lies.

(1) System accounts.

Uses of accounts
Account numbers.

(2) Normal user accounts.

User privileges
Special purposes.

(3) Special user accounts.

Special privileges
Special purposes

(4) Username selection.

Unique id for each and every user.

(5) Account lifetime.

(6) Password selection.

(7) Password expiration dates.

(8) Restriction of 'root', /su program or other privileged accounts to the console with printer.

(9) Control of dead accounts.

Procedure for removing all access rights.
Removal of suppliers default accounts.

(10) Standard to be used for user identities.

(11) Prevention of null passwords on system and user accounts. Configuration checking utilities such as ASPIDOS (available from DRA) or 'crack' (which will detect null, default and "common" passwords) will aid this.

(12) Authentication system.

f. System software.

(1) Software versions for use in special circumstances

Special versions of:
operating system
applications
protectively marked software
software with privileges
modified system components.

(2) Software change control. [CESG COMPUSEC Memo 11]

Certified system software
Method of amendment.

(3) System security copy as a master against which operational copies can be made or checked.

Create secure copy after updates.

(4) File and Directory access control system.

User permissions should be regularly checked.

(5) List of SUID programmes and reasons for use and the UID and GID assumed by each program.

(6) Restrictions on sensitive programmes.

eg. assembly level debugger.

(7) Warning that unauthorised software must not be used or loaded.

(8) Password generation/encryption algorithms should be CESG approved.

(9) Secure delivery of system software.

g. Auditing.

Using any audit software provided.

h. Security breach procedures (e.g. UNIRAS).

Notification to:

System software failure procedures.
Reporting unusual behaviour, system crashes.

j. Backup and restore of system.

k. Control of shared areas.

/tmp area.
/usr/tmp
/usr/spool/...
UMASK setting.

8. **Remote terminals and communications with workstations and systems**.

a. Classified working.

Applies to communications crossing secure boundary [BID/01/1].
State location of remote equipment.

b. Remote terminal security.

(1) Secure login.

Setting up terminals and accounts for best security.

(2) Secure logout.

Clearing screens
Any special logout processes.

(3) System password.

(4) Control of network logins.

Dial in.

c. Control of remote printers and print queues.

(1) Control of non-queued remote printers.

Limiting access by users.

(2) Control of remote printer queues.

d. Terminal session audit.

Logging all terminal access if possible.
Communications audit.

e. The "brandname" network.

Specific guidance on proprietary networks.

f. Control of network communications to other systems.

Distributed processing.
System network files eg hosts. equiv, -rhosts communications to be used
eg SENDMAIL, RLOGIN, TELNET, FTP, NFS, NIS.

Both annexes below can be repeated as many times as necessary to cover proprietary network architectures.

Each one need not be very long because it covers only the security aspects of management.

Annex A to Section 8.

This is general guidance to be supplied to the terminal user on how to keep the system secure while using a terminal.

g. Remote terminal user guide.

(1) Introduction.

(2) Remote login.

(3) Printing.

(4) The "brandname" network.

(5) Secure logout.

Annex B to Section 8.

How to set up a network to make it as secure as possible.

h. Network security.

(1) Configuring the host or node for the network.

(2) Network accounts.

(3) General.

i. Other Unix-specific network software.

Removal of EMAIL facility to outside world
Anonymous FTP
Use of FINGERD

j. Control of TCP/IP sockets.

9. **Accounting and audit**.

a. Introduction.

State which post(s) carries out these responsibilities.

b. Unix integrity.

Maintaining the assurance level.

c. Master backup.

Comparison of operating system files with a master copy.

Executable images in memory.

Periodic checks on what is running.

d. System monitoring.

Checks for user names in use, excessive privileges, number of device errors.

e. System auditing.

What should be selected if auditing of processes is available.

f. Security journals.

(1) Master console output.

Can it be recorded on paper?

(2) Accounting file.

Record of chargeable resources.

(3) Operators log.

Treatment of system log files.

(4) Intrusion database.

Some systems may record failed login attempts.

(5) Error log.

May be part of standard logs.

(6) User authorization file.

(7) Network authorization file.

(8) Rights database.

(9) Method of examining logs

eg AI (artificial Intelligence) system.

g. User Protection.

(1) Login messages.

Messages to a terminal before or after logging in.
Initial screen after logon:

'this is a secure system - no unauthorised access'

Date of the last successful login.

(2) File protection.

Checks that users should make on their files.

(3) Remedial action.

Action to be taken on finding discrepancies.

(4) User files.

UMASK settings to be used.
.rhosts, .netrc files within user areas.

(5) Access to 'root' should normally be via 'su' from an account unique to the individual user if more than one user has access to 'root', rather than a direct login to 'root' so that audit of who took superuser actions can be made.

h. Investigation of system crashes.

Check Lost+Found directories for sensitive files before opening to users.

i. Viruses

Action to be taken.

10. **Backup procedures**.

a. Disaster system copy.

Advice on using the dump and restore facilities.
Access control privileges to be checked on recovery.

11. **Emergency and breakdown procedures**.

a. Emergency shutdown procedures.

Few versions of Unix will have all these options.

(1) Standard shutdown.

(2) Emergency shutdown.

(3) System crash.

Deliberate crash for very fast halt.

12. **General operating procedure and guidance to users**.

a. Introduction.

This is a document for general guidance for all users to read.

b. Access to accounts.

(1) Login procedure.

The site's login procedure.

(2) Passwords.

Advice on how to choose passwords.

(3) Access to files.

File protection specific to the installation.

(4) Use of discs/file systems.

Restrictions
Use of.

c. Protectively marked printout.

Local instructions on handling.

d. Contacts for advice

(1) System.

(2) Software.

(3) Security.

ANNEX S TO

CHAPTER 3

SECURITY INSTRUCTIONS FOR SESSION PROCESSING MODE

1. A special case of Dedicated Mode is Session Processing Mode, which permits the use of a dedicated machine at different protective marking levels of data by using separate media sets.

2. If this method is to be used, the following additional paragraphs are to be included in the relevant Security Instructions (SyI):

paraX. The following sessions at different protective marking levels of data on separate media sets are currently defined:

a. Protective marking level 1, [list here the serial numbers of the set of media.]

b. Protective marking level 2, [list here the serial numbers of the set of media.]

(Use as many sub-paragraphs as there are protective marking levels.)

paraX+1. For each change between protective marking levels, the following procedures are to be followed:

a. Close down the current session, remove and secure media at this protective marking level and switch off all equipment for at least 15 seconds to allow volatile memory to purge.

b. Reconfigure the equipment as necessary to that permitted for the new protective marking level. (This will include the enabling/disabling of any remote link or T-switch as necessary.)

c. Obtain media for new protective marking level and reload all equipment in accordance with standard procedures, thus establishing a dedicated session at an alternative protective marking level.

This page is intentionally left blank

MEDIA MANAGEMENT

This page is intentionally left blank

CHAPTER 4

MEDIA MANAGEMENT

Introduction

0401. In an IT system, the volume and compactness of the information being processed, its ready accessibility, and the ease and speed of copying data, underlines the need for strict document security measures. Protectively marked information held on IT documents must be given a level of protection and control equivalent to that applied to protectively marked documents in paper form. The general principles of document security as described in other security documentation are to be applied. However, there are certain problems specific to IT systems and these are addressed below.

Definition

0402. The following are to be considered IT documents:

a. Paper including:

(1) Printed output, graphs, charts, flow-charts, plans, maps, drawings and computer logs.

(2) Punched paper tape.

b. Magnetic Media, including:

(1) Magnetic tapes.

(2) Cassettes and data cartridges.

(3) Removable magnetic disks.

(4) Floppy disks.

(5) Fixed magnetic disks.

(6) Non Volatile memory devices such as PROMS, EPROMS, and other programmable devices.

(7) Volatile memory such as printer and electronic typewriter memory.

c. Microform, computer output to microfilm and microfiche.

d. Ancillary materials, such as inked ribbons, carbon papers and backing sheets, which carry impressions or images of protectively marked information.

e. Optical Storage Devices such as CD ROM.

f. CCTV Screens.

g. In exceptional circumstances it may be necessary to treat VDUs as documents due to Screen 'burn in'.

Principles for Assessing the Appropriate Level of Protective Marking

0403. The principles for assessing the appropriate level of protective marking for information are covered in some detail in The Defence Manual of Security, Volume 1. The use of IT systems raises some additional concerns, both over information ownership and the aggregation of large quantities of data. Policy on such matters is at **Annex A**.

Segregation of National and International Defence Organization (IDO) Information

0404. Where it is necessary to process National and International Defence Organisation (IDO) information on a computer system, the following precautions are to be taken.

a. Where practicable, the two classes of information are to be stored on separate magnetic media.

b. Where the two classes of information have to be held on the same magnetic media, separation using a security functionality level of F-C2 or better is to be implemented. (See Chapter 15 for definition.)

0405. In the case of stand-alone PCs only, National and IDO information may be held on the same hard or floppy disk subject to the following conditions:

a. The two classes of information are kept in separate directories which are clearly labelled, or the disk is partitioned into more than one logical drive and the national and IDO information kept in separate drives. Each drive must be labelled.

b. IDO information is not to be electronically copied from such disks for release to the IDO concerned.

c. Disks are to be clearly marked as containing IDO information (eg 'Contains NATO data').

d. SyOPs are to contain specific instructions on the segregation of national and IDO information.

Markings

0406. Information which has been converted into machine-readable form and placed on IT documents is to be marked as if it were in plain language. Similarly data, e.g. numerical calculations, without headings or other identification is to be marked as if the headings were included.

0407. All IT documents are to carry their markings in eye-readable form, this is not to be lower than the highest marking of the data they bear (in most cases this is the highest protective marking processed on associated system). Colour coding, using labels or the issued media, is to be used to indicate the protective marking of documents.

Unclassified Documents needing Protection

0408. There are many unclassified documents associated with an IT system which need protection because access to them could lead to security safeguards being bypassed. These documents are to be identified by the ITSO as of security importance, and given appropriate physical protection. They could include:

a. The master copy of the controlling system software.

b. Programs used to test the security features of the controlling system software.

c. The master copies of utility programs.

d. Programs used to overwrite data storage media.

e. Application programs.

f. Directories of user files.

g. Lists of protectively marked files.

h. All access control information.

i. Stores of blank/unused magnetic media.

The Application of Protective Markings to IT Documents

0409. **General.** Every document must be clearly marked with its protective marking in plain language. In addition, a document or group of documents should be marked with a colour code as shown in other security documentation to denote its protective marking.

All storage media are to carry their protective markings and descriptors in eye-readable form throughout their lives unless downgraded in accordance with paragraph 0442.

0410. **Plain Language Documents.** These are to be marked in accordance with the provisions of other security documentation.

0411. **Printer Output.** The protective marking of printer output is to be marked in the centre of the top and bottom of every page. This can be achieved through a program instruction, by the use of pre-printed stationery, or manually. The protective marking may alternatively be shown, within an installation, by using coloured stationery. If coloured stationery is used, it is to conform to the protective marking colour code. The use of yellow paper is permitted to distinguish compartmented ("codeword") material from other material of the same protective marking level. The pages of TOP SECRET and SECRET output are to be page numbered either manually or automatically.

0412. **Punched Paper Tape.** Punched paper tapes are to be given a protective marking in plain language near the start and finish of the punching and at both ends of each piece of tape. Paper tape with pre-printed markings spaced at regular short intervals is also available from HMSO.

0413. **Magnetic Tape.** Marked labels should be fixed to:

a. The front flange of tape spools.

b. The edge of their protective canisters (if used).

c. The front of any suspension rings used to support the tape spools during storage.

d. Additionally, colour-coded tapes are to be used in accordance with the rules at **Annex B**.

Magnetic tape, including its leaders and trailers should **not** be inscribed physically or chemically with markings, nor have labels fixed directly to it. Labels should not be attached to the collars of self-loading magnetic tapes.

0414. **Cassettes.** Clear markings are to be applied to both:

a. The front and back faces of cassettes.

b. The spine of the plastic protective cassette box.

c. Additionally, colour-coded cassettes are to be used in accordance with the rules at **Annex B**.

0415. **Data Cartridge.** The tapes in cartridges which hold large quantities of data onwide magnetic tape are commonly inscribed by the manufacturer with a unique number which is visible (on the tape itself) through the outer casing. This number cannot be easily altered or erased and can serve as the registration number (para 0425 refers). Although the tape remains attached to the spool when the equipment is in operation, the spool becomes separated from its outer casing. The outer casings are interchangeable and external labels or markings should not, in any event, be applied to them. Additionally, colour-coded cartridges are to be used in accordance with the rules at Annex B.

0416. **Floppy Disks (Diskettes).** Floppy disks, or diskettes, are enclosed in a jacket which is sealed by the manufacturer and should never be opened. Markings are to be applied to labels fixed firmly to one side (whichever is specified by the manufacturer) of disk jackets. Markings should not be heavily inscribed with the label in position, since this could damage the floppy disk inside. If jackets are kept in paper or cardboard cases, markings are to be applied to the front and back of the cases. For SECRETand above, only pre-serial numbered, MOD supplied colour-coded diskettes are to be used unless dispensation has been obtained from the Accreditor(s). Colour-coded diskettes are to be used in accordance with the rules at **Annex B**.

0417. **Removable Magnetic Disks.** Removable magnetic disks and disk packs are to have markings:

a. Indelibly written in felt pen directly on the top of the disk or disk pack and also on the front for those that are used in PCs or portable systems. This marking should, wherever possible, be placed so that it can be seen whilst the item is in the drive.

b. Applied on labels fixed to the top and side of the plastic covers in which the disk or disk packs are normally stored or housed.

0418. **Fixed Magnetic Disks.** Fixed magnetic disks vary considerably in size and construction, and no general rule can be adopted other than that protective markings are to be applied to the case of the equipment containing the fixed magnetic disk and these items are then to be treated as items of classified equipment.

0419. **Microform (Microfilm and Microfiche) produced as IT System Output.**

a. **Microfilm.** Microfilm whether positive or negative, is to be given eye-readable markings, on a label or by perforations, on the leader and trailer of each length of film. These markings may be supplemented by coloured leaders and trailers. Canisters containing microfilms are to be given markings in plain language on a label fixed to their side.

b. **Microfiche.** Microfiches are to carry eye-readable markings on the title strip of each fiche. The markings are to transfer legibly to any copies made.

0420. **Optical Storage Devices.** Optical storage device containers should be markedwith indelible felt pen or have labels applied. On no account should any marking or label be applied to the device itself. MOD supplied colour coded CD-ROMs should be used in accordance with the rules in **Annex B**.

0421. **Other Devices.** Different types of memory are constantly being developed. They may present novel problems of applying protective markings and further advice is to be sought through the security staff.

IT System Document Control

0422. The objectives of document control are:

a. To enable an ITSO to know what protectively marked information is held and where, so that it can be accounted for at any time.

b. To restrict access to those with both security clearance and need to know.

c. To aid in the investigation of possible breaches of security. As with documents in a manual system, all computer documents are to be subject to appropriate registry procedures. There is to be no uncontrolled printing of protectively marked output.

0423. **General Principles.** The following principles are to be adhered to in all cases:

a. Detailed records are to be kept of the receipt and disposal of incoming IT documents, and media, and of the creation and dispatch of outgoing IT documents marked TOP SECRET and SECRET.

b. Records are to include the sender, protective marking and description of the information and details of the disposal to store, dispatch or destruction.

c. It will often be convenient to adapt records which would in any event be kept for work control and accounting purposes to cater for protectively marked information. Records need not be kept for temporary computer files i.e. those which do not survive the end of a run or session.

d. Checks and musters of computer documents are to be carried out in accordance with JSP 440 Volume 1. If for any reason it is not possible to conform to these instructions, the advice of the command security staff is to be sought.

e. As far as is practicable, the instructions on the registration of protectively marked documents in paper format are to be followed for computer documents. If, due to the nature or volume of computer documents these instructions cannot be complied

with, the command security staff and system Accreditors(s) are to be consulted on the detailed measures to be applied.

0424. **Recording of Protectively Marked Documents.** MOD Forms 102 are to be kept for at least five years from the date of closure (see Volume 1 Chapter 4 for details). Other records associated with document control are to be kept for a minimum of five years and longer if storage space permits. Registers are to be kept to indicate where information is held as follows:

a. All the media protectively marked SECRET or above held in the custody of a section or branch (probably in registration number order).

b. The title of the information stored on each magnetic medium.
NB: This is not always necessary, but where so can be abbreviated.

0425. **Unique Registration Number.** All removable media protectively marked SECRET and above require a unique eye-readable registration or identification number which is to be applied when first taken into use. The marking need be applied only in one place and is to be difficult to remove or alter without this being apparent. It is recommended as good management practice to register all media regardless of protective marking. Registration numbers are used to:

a. Provide each medium with a unique and permanent identification from the time of its first use until its destruction.

b. Enable its registration, movement and destruction to be recorded.

c. Aid auditing and spot checking.

d. Aid investigation into loss or compromise.

0426. **Removable Storage Media.** The following points should be kept in mind:

a. Media must retain the grading of the highest protectively marked information ever stored or processed until destroyed by an approved method or declassified by data destruction. (See **Annex C** for details of those items which can be declassified.)

b. Most media will contain no information on receipt and will be unclassified. It may be convenient, before bringing individual items into use, to allocate to all items the protective marking of the most highly protectively marked information which it will be allowed to carry.

Alternative Methods of Handling IT System Output

0427. **Introduction and Scope.** This section describes alternative methods for handling output from computer systems to those generally adopted when implementing security regulations:

a. The implication of running Multi-Level and Compartmented Modes of Secure Operation is that the system is trusted to maintain security and need-to-know. It may do so by labelling information, and this can form the basis for applying security markings to output in accordance with departmental security instructions. Hence, Multi-Level and Compartmented systems are not discussed further in this section. The implication for System High and Dedicated Modes of Secure Operation, however, is that little or no such trust in upholding separation is placed on the system. Hence all information on the system has to be treated as potentially of the highest level of protective marking and/or category on the system.

b. Too rigid an implementation of this policy has led to output from Dedicated or System High systems being routinely protectively marked as if it were of the highest protective marking or category. It may then have to be recorded in a MOD Form 102. If bearing a protective marking label higher than its actual content, it should be downgraded, and this event too has to be recorded in the MOD Form 102. In situations where very little of the information on a system is at the highest protective marking, the effort involved in following such a policy may be immense. This section describes alternative methods for protectively marking printed or magnetic output. Other forms of output, such as direct links to other IT systems, electronic mail, etc., are to be treated as for the highest level of information the system stores, processes, or retains.

0428. **Printed and other human-readable output.** Plain printed text or other output, the nature and meaning of which can be readily assessed by the originator, is to be protectively marked according to its content. This is in line with the general requirements of other security documentation. Format, legibility, and volume of output are to be within reasonable bounds. Technical, schematic or large volumes of data are not suitable for such uncontrolled output and should therefore be protectively marked as for the highest protective marking the system processes. The output should be inspected to ensure that the security protective marking is correct.

0429. **Output to magnetic media.**

a. National technical security advice is that magnetic media is always to attract the highest protective marking that has ever been held on it. Also, IT systems work most efficiently by transferring blocks of data between the central processor and any magnetic media drives, regardless of how much of the blocks contain unrelated data, possibly at a higher protective marking. Small IT

systems in particular occasionally use media for temporary storage, often without the knowledge of the user.

b. Accordingly, all magnetic media mounted on IT systems must be treated as for the highest protective marking on that system, and colour-coded diskettes have been introduced to help implement this rule. Where, however, there is a need to produce magnetic output from a system at some lower protective marking than that of the system, for example for transferring data between systems, the following rules are to be followed:

(1) The procedures for handling all output are to be incorporated into the system Security Operating Procedures (SyOPs) and submitted for approval by the appropriate security authority prior to using the system. The agreed SyOPs are to be brought to the attention of all users on a regular basis.

(2) It is preferable that previously unused media be used, but old media may be used provided it has never attracted a protective marking higher than that of the intended output. Disks or diskettes are first to be formatted, using a system at the target protective marking or less. Following transfer of the output data, the media is then to be write-protected before following the next step.

(3) The content of the media is then to be verified on the output system, or one running at an equivalent protective marking, using suitable utilities software which will display the entire contents in block format. The originator is to inspect the contents and assess the protective marking of all the information found. The media is then immediately to be removed and given the appropriate security marking, if any, and thereafter treated in accordance with existing security regulations.

c. **Summary.** With the prior approval of the Accreditor, it may be permissible for information on Dedicated or System High IT systems to be output at a lower protective marking than that of the system itself. This upholds the general principle that information is to be protectively marked according to its content. The methods to be used are to be documented in the systems' SyOPs, approved by the Accreditor, and then promulgated to all users.

Control Procedures for Protectively Marked IT Systems, Hard Copy Output

0430. The following is to be implemented with regard to hard copy output that requires protective marking:

a. Protectively marked hard copy output is to be delivered to, or collected by, the originator or a person authorized by the originator.

b. Programs (whether system software or user programs) producing protectively marked hard copy output are to where possible:

(1) Print the protective marking at the top and bottom of each page.

(2) Page number the pages of TOP SECRET and SECRET print outs.

(3) Total number of pages.

c. Where programs do not provide the facilities at b above, a manual system must be introduced.

d. Hard copy output is to be held in an approved manner from the time it leaves the printer until it is received by the originator, is dispatched by approved means, or destroyed.

0431. **Hard Copy Output from Program Testing.** Programs are to be tested, as far as possible, using unclassified dummy data. When it is necessary to use live protectively marked data, the hard copy output is to be treated as protectively marked. Hard copy output from test runs is not to be allowed to accumulate, but is to be destroyed when no longer required.

0432. **Graphs, Charts, Drawings etc.** Output from other peripherals, such as plotters, which produce eye-readable material should be dealt with in the same way as textual print.

0433. **Computer Output to Microform (COM).** User identification and job identification should be shown on both microfilm and microfiche in eye-readable form. The frames of TOP SECRET and SECRET output are to be serially numbered, and the last frame indicated. Tight physical control is to be exercised over the COM devices (microfilm/microfiche), including checks on film waste and film counters. Where counters are available then a record is to be kept of the serial numbers and the jobs they relate to. When duplication of the film is necessary, a close check is to be made on the authority to reproduce, on material used and on film counters. The use of non-re-settable or locked counters should be considered.

0434. **Paper Tape.** The output from paper tape punches presents additional problems in that it is more difficult to identify the protective marking of the content. The following measures will be necessary. Where possible the program or controlling system software should punch, at the beginning of the paper tape, information on the identity of the job, its owner and the security protective marking of the output. This should be carried out in plain language. However, if this is not possible, means must be readily available for the interpretation of the information as an essential part of the output identification procedure.

0435. Treatment of protectively marked documents or information no longer required. Good security requires the amount of protectively marked information to be kept to a minimum. Protectively marked information is to be destroyed, erased or over-written as soon as it is no longer required. The ITSO is to regularly check to verify that protectively marked information is not being retained unnecessarily.

Storage and Custody of Protectively Marked Documents

0436. All protectively marked IT documents, as described above, and ancillary materials are to be stored, when not in use, to approved standards as described in JSP 440 Volume 1.

0437. Where it is necessary to restrict access to a particular type of information to cleared personnel with a strict need-to-know, it may be necessary to provide security containers within a secure room. This includes unclassified documents requiring protection. Provision must also be made for the separate storage of cryptographic key material where applicable.

0438. Back-up copies of protectively marked files stored at a different location are to be protected in accordance with the protective marking of the information stored.

0439. Data stored on magnetic media may be encrypted to prevent disclosure. Provided that the encryption process and associated procedures have been approved by HMG, the encrypted data may be regarded as unclassified. However, security advice is essential and there are to be no compromising identification details or markings on the media itself. Even when the data has been encrypted, the media may still require a degree of physical protection against theft or sabotage.

0440. **Custody of Unclassified Documents Requiring Protection.** Documents which are unclassified but which give access to protectively marked data are to be given protection at least equivalent to the level of the highest protective marking of data processed on the system. When recorded on removable media, this media is to be kept under secure conditions when not in use, and is not be loaded unless the agreed SyOPs are in force.

0441. Wherever passwords are printed or written down, they are to be given protection commensurate with the highest protective marking processed by the system to which they refer. They should normally be stored under the same conditions as combinations for manifoil locks; i.e. sealed in an envelope with clear instructions stating the conditions under which it can be opened.

Erasure of Protectively Marked Data on Computer Storage Media

0442. Redundant protectively marked data is to be erased. Secure erasure defines a more thorough process than deletion and may comprise of the following depending on the security risk assessment:

a. **Clearing**. A process, which overwrites the data, making it unrecoverable through a systems interface (e.g. keyboard). Essentially it gives only need to know protection;

b. **Purging**. The eradication of data such that it can be expected to withstand recovery, even under an attack employing sophisticated, specialised hardware. Two types of erasure are permissible. This permits the release of the media from Government custody and is a more stringent procedure than clearing.

Details of the rules and procedures for clearing and purging are at **Annex C**.

0443. **Accidental or Malicious Erasure of Magnetic Media.** Safeguards against the accidental or malicious erasure of magnetic media in IT Systems or installations are provided by:

a. Installation operating standards.

b. System security features provided by media manufacturers, e.g. write-protect tabs, and by software designers.

c. Where protectively marked data has been accidentally or maliciously erased from magnetic media, system operating procedures may be at fault. An investigation must be made to establish how the data was lost in order to take appropriate precautions against a recurrence. Contingency plans will normally provide for the reconstruction of magnetic data which may have been erased.

0444. Magnetically recorded data may be affected by extraneous electromagnetic or magnetic fields. The introduction of strong magnets or any unauthorized electrical equipment into an installation is to be forbidden. For the same reason suitable precautions are to be taken when magnetic media is in transit, e.g. railway power rails.

0445. In all cases of accidental or malicious erasure of magnetic media, an investigation is to be conducted to establish the cause and to take remedial action. Where malicious damage is suspected, the security staff are to be informed through the chain of command.

0446. **Non-Government Media.** Special care is to be taken if it is intended to hire or borrow computer equipment, for example a personal computer or a disk drive unit. Any rented equipment that has been used for protectively marked work is not to be returned

unless all magnetic storage devices, including fixed disks, have been removed and retained or destroyed, or declassified if applicable, before returning the equipment. It is **NOT** sufficient to over-write the disk several times see Annex C.

0447. **Physical Destruction.** Redundant protectively marked computer storage media is to be destroyed (preferably on site) as protectively marked waste by an approved method if it cannot be declassified by purging or cleared for re-use. It should be recorded as having been destroyed as required by the security instructions. Whenever possible, protectively marked storage media is to be erased or over-written before the media is placed in custody ready for destruction.

0448. The Security Equipment Assessment Panel (SEAP) Catalogue contains a list of approved commercial facilities that can be used for the destruction of protectively marked waste.

This page is intentionally left blank

ANNEX A TO

CHAPTER 4

THE PROTECTION OF INFORMATION HELD ON COMMUNICATIONS AND INFORMATION SYSTEMS

General Principles

1. The protection of information is covered in some detail in other volumes of the Defence Manual of Security; the purpose of this Annex is to consider some of the implications, particularly when information is held on CIS.

2. a. In general terms, all information has some value whether that represents the value of resources spent on its collection and recording or the value that can be gained from its exploitation. When assessing its value a judgement has to be made on the degree of damage likely to be caused to government assets caused by **compromise**. The cause of compromise can be broken down into four general groups:

(i) Disclosure.

(ii) Theft.

(iii) Destruction.

(iv) Tampering.

b. Based on an assessment of the outcome of such a compromise all assets, whether information or physical items are allocated a **Protective Marking**. A table setting out these criteria is at Appendix 1 to this Annex.

c. Also, in general terms, information can be owned and the owner can and should be responsible for determining its level of protection (see paragraph 5 below). This includes information released to the UK Government by international agreement or on a commercial basis.

3. Information concerned with the business of Government or Service activities, which a Crown Servant or a Government contractor has by his or her position as such, is deemed to be "official" and the communication of any "official" information to any

person (other than one authorised to receive it) is expressly forbidden by the Official Secrets Act. The originator of "official" information is not, therefore, the owner of that information. The rules for the protection of "official" information are based on the allocation of a protective marking, the criteria for which are set out in other security publications. The authority to allocate a protective marking is limited to certain ranks and appointments, although in an emergency the originator of a document of any rank may authorize any protective marking provided the definitions laid down are used and can be justified.

National Caveats

4. Instructions for the use of national caveats are promulgated in other security publications but some important extracts are set out here with regard to the two core national caveats.

a. **UK EYES ONLY.** Information bearing the national caveat UK EYES ONLY is not to be released to any other country and, within UK Government Service, is strictly to be confined to those staff as detailed in JSP 440 Volume 1. It should be used sparingly. Originators are reminded that indiscriminate use can lead to transmission and custody difficulties and it should only be used where there is a real risk that information, whose uncontrolled disclosure would cause real damage to the UK, may inadvertently or unwittingly be disclosed to those who are outside the listed categories. It should not be used where the originator wishes to indicate that information is not to be released to a particular country. In such cases this should be indicated in the text eg "This information is not to be passed to the Ruritanians"

b. **UK EYES DISCRETION.** Information bearing the national caveat UK EYES DISCRETION is not to be released to any other country, nor to any other than a person in the above category or, on a discretionary basis to a slightly wider category listed in JSP 440 Volume 1. Information may be released by originators or owners of the information only to those detailed in Chapter 16 of Volume 1. In marking material with this caveat, the originator is delegating his release authority (including that of the PROTECTIVE MARKING) to the named recipient(s) (ie a named individual or specific post). It may, therefore, at the named recipient's discretion, be released to other UK and dual nationals (provided one nationality is British) and exchange/integrated officers and officers on attachment to UK Armed Forces, only where the conditions detailed in Chapter 16 of Volume 1 are met. It thus provides flexibility for named recipients to make a valued judgement on further dissemination, immediately, and without reference to the originator of the information but having regard to the release of information table in JSP 440 Volume 1 Chapter 11.

Mandatory Protective Marking Levels

5. In some cases, information on a particular subject will attract a mandatory protective marking. Mandatory degrees of protection are also associated with projects covered by codewords of various kinds and statistical records. In these cases the originator of an item of information may not protectively mark it lower than the mandatory prescribed level. In Information Technology (IT) terms, the degree of protection is "owned" by the authority setting the mandatory level and the originator is the "holder" of that protective marking. This is an extension to the existing rule in other security documentation whereby holders of documents protectively marked CONFIDENTIAL and all documents protectively marked SECRET or higher have to consult the originator if they consider a regrading is necessary.

Aggregation of Information

6. The sensitivity of information is greatly influenced by the context in which it is, or can be viewed. The aggregation of information and its exploitation by electronic processing is the basis of the IT revolution. The security of a set of information may attract a higher degree of protection than an individual record and the originator of a piece of information may be unaware of its ultimate sensitivities. For instance the reliability of a fleet of vehicles is of higher sensitivity than for a single vehicle. If that fleet could be more closely defined as essential to an operational theatre, then it would be higher still. The System Manager, acting on behalf of his command authority, may need to take advice on the degree of protection necessary for such aggregated information and to assign a higher mandatory level to a computer document after processing. There may also be a need to anticipate an overall degree of protection for the CIS which allows for aggregation of user data. This may be particularly important when considering the level of compromise which might result from the destruction or tampering of a database. In some cases it may be possible to employ the opposite effect of decreasing the security application of information by removing the appropriate context, such as is used in "veiled" speech.

This page intentionally left blank

ANNEX B TO

CHAPTER 4

COLOUR-CODED MEDIA

Introduction

1. Diskettes and other items of storage media coloured green, pink, or red, are available from the MOD ICS catalogue. The principles for using diskettes are set below. Each disk uniquely numbered and indelibly marked 'MOD' and should be used as follows:-

Disk colour	Only to be used on machines which are cleared up to and including:
Non colour-coded	Unclassified/RESTRICTED
Green	CONFIDENTIAL
Pink	SECRET
Red	TOP SECRET

2. This media is to be used for computer, word-processing, and other Information Technology (IT) equipment which processes, stores, or forwards information protectively marked CONFIDENTIAL or above. Non colour-coded diskettes are only to be used on Unclassified or RESTRICTED IT equipment.

3. Hence, subject to paras 4 and 5 below, diskettes are only to be used if they are of the colour appropriate to the highest protective marking of information for which the equipment has been cleared (see table above). This also applies to diskettes which contain programs or system software.

4. When it is necessary to import data using a diskette of lower protective marking, the write-protect mechanism is to be used to prevent inadvertently writing more highly protectively marked data on to the diskette, and the rules which describe such use are to be included in the equipment's Security Operating Procedures (SyOPs).

Equipment with no Fixed Disks

5. Where equipment has already been approved for use at different protective markings at different times (dedicated sessions), then the appropriately coloured, or non colour-coded, diskette may be used provided the equipment has first been purged of more highly protectively marked data by an approved method. Approval for such use of

IT equipment, and of the instructions contained in the SyOPs, is to be obtained through the security chain of command.

Implementation

6. Each colour coded diskette has a unique serial number. Each pack of 10 contains consecutive numbers, displayed on the wrapping, and may be regarded as unclassified until the packaging is broken. Base/Unit Security Officers are to record (by serial number) the issue of packs to users, since each diskette is to be individually accounted for. This will help security staff to trace the origin of misplaced media.

7. Once taken into use (as soon as the wrapping is broken) the individual items are to be treated as protectively marked documents: they are to be labelled and recorded as appropriate. When recording the diskette in a classified (or other, appropriate) document register, the unique serial numbers printed on the diskettes are to be used.

8. There may be a great number of protectively marked non colour-coded diskettes which need replacing. Staff are reminded that copying of data is to be performed on appropriately cleared equipment, and that the copying of protectively marked documents (including diskettes) is to be recorded in an appropriate manner.

9. Unless the protectively marked non colour-coded diskettes which have been replaced or superseded meet the criteria laid down in Chapter 4, they may not be de-classified nor down-graded but must be physically destroyed by an approved method.

N.B. BEFORE PHYSICALLY DESTROYING OR DE-CLASSIFYING ANY NON COLOUR-CODED DISKETTES CHECK FIRST THAT ANY COPIES WHICH HAVE BEEN MADE ARE READABLE.

10. The items listed below are now also available in a colour-coded range from the MOD ICS catalogue and are mandated to be used, retrospective action is not required but all new buys must be colour coded. The principles for usage are as given for diskettes.

a. **Colour Coded Media**

DC Data Cartridges
Mini Data Cartridges
4mm DAT Cassettes
8mm DAT Cassettes
8mm Exabyte Cartridges
3480 Series Archival Grade Cartridges
Archival Grade Reel to Reel Tape
Recordable CDs

ANNEX C TO

CHAPTER 4

ERASURE FOR REUSE OR DISPOSAL

Introduction

1. When IT equipment becomes surplus to requirements care must be taken to ensure that its disposal does not expose any protectively marked material which it has processed or stored, to an unacceptable risk of compromise. This guidance applies to all types of computer storage media: magnetic disks and tapes, optical disks, magnetic computer memory and semi-conductor memory. Where it is impractical to separate the computer storage media from the equipment of which it is a part, the guidance should be taken to apply to the whole equipment.

2. This Annex provides guidance to the owners of Communications and Information Systems on the security aspects of reuse or disposal of protectively marked computer storage media as an alternative to destruction. The "deletion" of computer files and data generally only suppresses that information from immediate view, and makes the area of storage available for overwriting. The "deleted" information can usually be recovered with minimal expertise using COTS utility software. Secure erasure of protectively marked-marked data, requires a more deliberate erasure procedure to a specified overwriting or degaussing standard, which will positively verify that secure erasure has occurred.

3. The physical properties of storage media are such that, even after a thorough overwriting, minute electrical or magnetic effects may remain. However it is a technically complex operation, requiring specialist equipment and considerable resources, to recover usable data.

Threats

4. The threat of protectively marked data being compromised is lowest when storage media is released for re-use within the same or equivalent security environment. The threat is significantly increased when storage media is released outside the secure environment. Disposal of storage media on the open market, by resale or recycling, increases the potential for data falling accidentally into the wrong hands or being positively targeted. The threat may relate to the attractiveness of the data to an attacker.

5. **Attractive data** will include:

a. All data protectively marked TOP SECRET and SECRET;

b. Data with especially sensitive need-to-know considerations (includes STRAP material);

c. Cryptovariables;

d. All data with UK Eyes caveats.

Secure Erasure

6. Secure erasure defines a more thorough process than deletion and may comprise of any of the following depending on the security risk assessment:

a. **Clearing**. A process, which overwrites the data, making it unrecoverable through a systems interface (e.g. keyboard);

b. **Purging**. The eradication of data such that it can be expected to withstand recovery, even under an attack employing sophisticated, specialised hardware. It is not possible to give categorical assurance that purging will be sufficient in all circumstances. However, a successful attack is likely to be both technically difficult and expensive and the risk can often be dismissed, unless the data is likely to be particularly attractive to the attacker;

c. **Destruction**. Physical destruction of the media, which may be preferred when the residual risk after purging is considered unacceptable.

7. The success of the erasure should be positively verified. If there is a large quantity of storage media for re-use, it may be decided that verification of a sample, rather than a whole batch, is sufficient to manage the risk.

Secure Erasure Standards

8. The Security Equipment Assessment Panel (SEAP) is an organisation of the Cabinet Office responsible for physical security equipment. The SEAP catalogue of Security Equipment (CSE) offers approved degaussing equipment for the secure erasure of media.

9. The degaussing process detailed in the equipment user manual is to be strictly followed. After degaussing, a representative sample of all degaussed media that previously contained protectively marked information is to be checked, by attempting to read data from the degaussed medium, to give confidence that erasure has taken place. After degaussing, media is considered to be Unclassified and is to be marked accordingly.

10. Equipment meeting the SEAP Degaussing Standard Class 1 is acceptable for secure erasure of media that has held RESTRICTED and Degaussing Standard Class 2 is acceptable for secure erasure of media that has held CONFIDENTIAL and above.

11. Staff should be aware that **degaussing might not be fully effective on some of the modern high-density back-up storage media**. The approved equipments are not suitable for degaussing magnetic tapes and cartridges with coercivity greater than 1700 Oersteds. When purchasing magnetic media, the supplier will be able to provide information on its coercivity.

12. COTS overwriting products, which meet the baseline and enhanced standards set out in CESG Infosec Memorandum No.7, must be used for secure erasure of media.

13. The **Baseline Standard** requirements for COTS overwrite utilities are:

a. The overwriting and verification applications shall run from a bootable floppy disk or CD-ROM;

b. Both overwrite and verification applications shall report the actual disk capacity to be overwritten. (The actual disk capacity should be ascertained, possibly by calculation, prior to overwriting since BIOS, FDISK, CHKDSK and Windows etc, cannot be relied upon to accurately report disk capacity);

c. The overwriting application shall write a single bit pattern to all addressable areas;

d. The verification application shall generate a report that all addressable areas have been overwritten;

e. The verification application shall report any bad or unusable sectors that cannot be overwritten;

f. Verification of successful secure erasure is recommended;

14. The **Enhanced Standard** requirements for COTS overwrite utilities are:

a. The overwriting and verification applications shall run from a bootable floppy disk or CD-ROM;

b. Both overwrite and verification applications shall report the actual disk capacity to be overwritten. (The actual disk capacity should be ascertained, possibly by calculation, prior to overwriting since BIOS, FDISK, CHKDSK and Windows etc, cannot be relied upon to accurately report disk capacity);

c. The overwriting application shall write a single bit pattern to all addressable areas, then its complement for three overwrite cycles, then finally a random pattern (i.e. 7 overwrites);

d. The verification application shall generate a report that all addressable areas have been overwritten;

e. The verification application shall report any bad or unusable sectors that cannot be overwritten.

f. Verification of successful erasure shall be carried out for all clearing and purging instances;

15. Annex A to CESG Infosec Memorandum No. 7 sets out compliance specifications for the baseline and enhanced standards, which COTS secure overwriting products, should meet.

Re-use Within the Same Secure Installation

16. When storage media is to be reused within the same (or equivalent) security environment, but by a different user, all protectively marked data should be removed. Media that has been cleared for re-use retains the highest protective marking of information stored on it since it was new (or since it was last purged).

17. **Semiconductor Memory and Magnetic Media**. For clearing of data up to and including CONFIDENTIAL, overwriting products that meet the Baseline Standard shall be used.

18. For clearing of SECRET and TOP SECRET data, overwriting products that meet the Enhanced Standard shall be used.

19. A trusted computer system may have a mechanism that enforces an object re-use policy, which ensures that non-privileged users cannot recover another user's data from recycled storage media. Systems that have an object re-use mechanism that is assured (that is to say the implementation has been evaluated by an independent, accredited, evaluation facility), meet the Baseline and Enhanced Standard requirements for secure erasure for all protective markings.

20. Low level formatting refers to overwriting below the level of the operating system. These formatting facilities tend to be manufacturer specific and may not be readily available to users. Where it is possible to perform a low-level format, and secure erasure can be positively verified, this will meet the Baseline Standard requirements for secure erasure.

21. **Optical Disks**. Re-writeable optical disks that have held data up to and including CONFIDENTIAL may be cleared in accordance with the Baseline Standard.

Read-only and recordable (Write Once Read Many) optical disks cannot be cleared and must be destroyed.

Re-use in Another Secure Installation

22. As above, the media retains the same protective marking. However, it is good practice to purge the media so that it may be re-used at any protective marking.

23. Removable storage media, which is to be used in another secure installation, should be treated as if it were being disposed of, and shall therefore be purged using procedures at either Baseline or Enhanced Standard as appropriate.

Disposal Outside of Secure Environments

24. The Disposal Sales Agency operates Marketing Agreements with commercial companies for the collection and sale of surplus marketable IT equipment.

25. Before storage media that has held protectively marked data is released outside the secure environment, it should be purged, after which it may be considered not to require a protective marking.

26. **Semiconductor Memory and Magnetic Media**. Storage media that has held attractive data (see para 5) should not be disposed of outside the United Kingdom. If it is located outside the United Kingdom and cannot be returned, then the only practical solution is destruction.

27. Before releasing storage media within the United Kingdom, that has stored held attractive data other than SECRET, whether for disposal, repair, exchange or return after hire, advice should be sought from the national security authorities, through the appropriate PSyA security staff and D Def Sy.

28. When releasing storage media that has held other protectively marked data, for re-cycling, resale or destruction, local security staff should be satisfied that it has been properly purged and therefore no longer needs to be protectively marked.

29. For purging of data up to RESTRICTED, overwriting products that meet the Baseline Standard should be used. Alternatively the media may be degaussed using equipment meeting SEAP Degaussing Standard Class 1.

30. For purging of data up to SECRET, overwriting products that meet the Enhanced Standard should be used. Alternatively the media may be degaussed using equipment meeting SEAP Degaussing Standard Class 2.

31. If hard disk drives are to be degaussed, the drive assembly must be removed from its housing or caddy to expose the platters before degaussing. If it is not possible to remove the drive, overwriting or destruction are the only options.

32. In some circumstances, where particularly sensitive or attractive data (see para 5) has been stored, then destruction may be considered the only secure disposal option. Destruction may also be preferred in other cases as representing the most economical security measure, given the relatively low cost of magnetic media).

33. **Optical Disks**. Re-writable, read-only, recordable (Write Once Read Many) optical disks shall be destroyed in accordance with the SEAP guidance.

Repair and Exchange

34. Advice should be sought through appropriate PSyA security staff from the national security authorities before any unserviceable or faulty media that has held attractive data (see para 5) is put forward for repair or exchange.

35. Leased equipment containing non–removable storage media should have the media purged before it is returned to the vendor.

36. Faulty or unserviceable storage media should be purged before repair or exchange. If a disk platter has unusable tracks or sectors, where protectively marked information may have been stored, and these areas cannot be overwritten, it should be degaussed or destroyed. If there is reason to doubt the thoroughness of the overwriting or degassing process, then the advice of the appropriate PSyA security staff should be sought before seeking exchange or repair.

37. Repair or exchange of computer storage media should be carried out either in situ within the secure controlled site, or at a suitable List X facility. In extreme circumstances, where on-site/List X facilities are not available, the faulty media may need to be escorted by suitably cleared/qualified personnel to a non-List X contractor's premises to oversee the repair or exchange. The repair and return of storage media should be supervised at all times.

Disposal by Destruction

38. Protectively marked IT equipment and media can be disposed of by using an approved method of destruction. MOD and Government approved commercial facilities exist to undertake destruction. The SEAP catalogue contains a list of approved commercial facilities that can be used for the destruction of protectively marked IT equipment and media. The advice of the appropriate PSyA security staff should be sought regarding requirements for destruction of protectively marked IT equipment and media.

Security Approval

39. The authority of the ITSO is to be sought prior to the reallocation or disposal of protectively marked IT equipment.

Erasure Requirements

40. The erasure requirements for different types of media for re-use, disposal and repair/exchange are set out in **Appendix 1**.

This page intentionally left blank.

APPENDIX 1 TO ANNEX C TO

CHAPTER 4

ERASURE OF PROTECTIVELY MARKED COMPUTER STORAGE MEDIA

MAGNETIC DISKS	**RE-USE**		**DISPOSAL**		**REPAIR/EXCHANGE**	
	Baseline Standard	*Enhanced Standard*	*Baseline Standard*	*Enhanced Standard*	*Baseline Standard*	*Enhanced Standard*
BERNOULLI CARTRIDGES	Overwrite[1], or low-level format, or use any approved degausser[3]	Overwrite[2], or use any approved Class 2 degausser[3]	Overwrite[1], or use any approved degausser[3], or destroy[4]	Overwrite[2], or use any approved Class 2 degausser[3] or destroy[4]	Overwrite[1], or use any approved degausser[3]	Overwrite[2], or use any approved Class 2 degausser[3]
FLOPPY DISKS	Overwrite[1] or low-level format, or use any approved degausser[3]	Overwrite[2], or use any approved Class 2 degausser[3.]	Overwrite[1], or use any approved degausser[3], or destroy	Destroy[4]	Destroy[4]	Destroy[4]
FIXED HARD DISKS	Overwrite[1] or low-level format	Overwrite[1]	Overwrite[1], or destroy[4]	Overwrite[2], or destroy[4]	Overwrite[1]	Overwrite[1]
REMOVABLE HARD DISKS	Overwrite[1] or low-level format, or use any approved degausser[3]	Overwrite[2], or use any approved Class 2 degausser[3]	Overwrite[1], or use any approved degausser[3] or destroy[4]	Overwrite[2], or use any approved Class 2 degausser[3], or destroy[4]	Overwrite[1], or use any approved degausser[3]	Overwrite[2], or use any approved Class 2 degausser[3]

Notes:

1. In accordance with the Baseline overwriting Standard.
2. In accordance with the Enhanced Overwriting Standard
3. All degaussers must comply with the SEAP standards
4. Destroy – Disintegrate , incinerate, pulverise, shred or melt.

MAGNETIC TAPES	**RE-USE**		**DISPOSAL**		**REPAIR/EXCHANGE**	
	Baseline Standard	*Enhanced Standard*	*Baseline Standard*	*Enhanced Standard*	*Baseline Standard*	*Enhanced Standard*
TYPE I (up to 350 Oe)	Any approved degausser[1]	Any approved Class 2 degausser[1]	Any approved Class 1 or 2 degausser[1], or destroy[2]	Any approved Class 2 degausser[1], or destroy[2]	Any approved Class 2 degausser[1]	Any approved Class 2 degausser[1]
TYPE II (up to 750 Oe)	Any approved degausser[1]	Any approved Class 2 degausser[1]	Approved Type II, IIA or III Class 1 or 2 degausser[1], or destroy[2]	Approved Type II, IIA or III Class 2 degausser[1], or destroy[2]	Approved Type II, IIA or III Class 2 degausser[1]	Approved Type II, IIA or III Class 2 degausser[1]
TYPE IIA (up to 900 Oe)	Any approved degausser[1]	Any approved Class 2 degausser[1]	Approved Type IIA or III Class 1 or 2 degausser[1] or destroy[2]	Approved Type IIA or III Class 2 degausser[1], or destroy[2]	Approved Type IIA or III Class 2 degausser[1]	Approved Type IIA or III Class 2 degausser[1]
TYPE III (up to 1700 Oe)	Any approved degausser[1]	Any approved Class 2 degausser[1]	Approved Type III Class 1 or 2 degausser[1], or destroy[2]	Approved Type III Class 2 degausser[1], or destroy[2]	Approved Type III Class 2 degausser[1]	Approved Type III Class 2 degausser[1]

Notes:

1. All degaussers must comply with the SEAP standards.
2. Destroy – Disintegrate, incinerate, pulverise, shred or melt.

MAGNETIC MEMORY	**RE-USE**		**DISPOSAL**		**REPAIR/EXCHANGE**	
	Baseline Standard	*Enhanced Standard*	*Baseline Standard*	*Enhanced Standard*	*Baseline Standard*	*Enhanced Standard*
MAGNETIC BUBBLE MEMORY	Overwrite[1], or degauss [3 or 4]	Overwrite[2], or degauss[4]	Overwrite[1], degauss[3 or 4], or destroy[5]	Overwrite[2], or degauss[4], or destroy[5]	Overwrite[1], degauss[3 or 4]	Overwrite[2], or degauss[4]
MAGNETIC CORE MEMORY	Ovewrite[1], or degauss[3 or 4]	Overwrite[2], or degauss[4]	Overwrite[2], degauss[4], or destroy[5]	Overwrite[2], or degauss[4], or destroy[5]	Overwrite[1], degauss[3 or 4]	Overwrite[2], or degauss[4]

Notes:

1. In accordance with the Baseline Overwriting Standard
2. In accordance with the Enhanced Overwriting Standard
3. Use a SEAP approved Class 1 (Lower) degausser.
4. Use a SEAP approved Class 2 (Higher) degausser
5. Destroy, Disintegrate, incinerate, pulverise, shred or melt.

SEMI-CONDUCTOR MEMORY	RE-USE		DISPOSAL		REPAIR/EXCHANGE	
	Baseline Standard	*Enhanced Standard*	*Baseline Standard*	*Enhanced Standard*	*Baseline Standard*	*Enhanced Standard*
RAM	Overwrite[1]	Overwrite[2]	Overwrite[1] then remove all power, or destroy[7]	Overwrite[2] then remove all power, or destroy[7]	Overwrite[1] then remove all power	Overwrite[2], then remove all power
DRAM	Overwrite[1] or remove all power	Overwrite[2] then remove all power	Overwrite[1] then remove all power, or destroy[7]	Overwrite[2], or destroy[7]	Overwrite[2], then leave powered-up for 72 hours	Overwrite[2,3], then leave powered-up for 72 hours
EPROM	UV erase[4]	UV erase[5]	UV erase[4], then Overwrite[1], or destroy[7]	UV erase[5] then Overwrite[2] or destroy[7]	UV erase[4], then Overwrite[1]	UV erase[5] then Overwrite[2]
FLASH EPROM	Chip erase[6] or Overwrite[1]	Chip erase[6] then Overwrite[2]	Chip erase[6] then Overwrite[1], or destroy[7]	Chip erase[6] then Overwrite[2], or destroy[7]	Chip erase[6] then Overwrite[1]	Chip erase[6] then Overwrite[2]
EEPROM	Chip erase[6] or Overwrite[1]	Chip erase[6] then Overwrite[2]	Chip erase[6] or Overwrite[1] or destroy[7]	Chip erase[6] then Overwrite[2] or destroy[7]	Chip erase[6] then Overwrite[2,3]	Chip erase[6] then Overwrite[2,3]
OTHER DEVICES	Destroy[7]	Destroy[7] or seek CESG advice	Destroy[7] or seek CESG advice	Destroy[7] or seek CESG advice	Destroy[7] or seek CESG advice	Destroy[7] or seek CESG advice

Notes:

1. In accordance with the Baseline Overwriting Standard
2. In accordance with the Enhanced Overwriting Standard
3. Each overwrite shall reside in memory longer than protectively marked data.
4. Ultra-Violet (UV) erase in accordance with manufacturers' recommendations.
5. Increase UV erase time by a factor of 5
6. Full chip erase as per manufacturers' data sheets.
7. Destroy – Disintegrate, incinerate, pulverise, shred or melt.

OPTICAL DISKS	**RE-USE**		**DISPOSAL**		**REPAIR/EXCHANGE**	
	Baseline Standard	*Enhanced Standard*	*Baseline Standard*	*Enhanced Standard*	*Baseline Standard*	**Enhanced** *Standard*
RE-WRITABLE CD-RW DVD-RAM DVD-RW	Erase[1]	Destroy[3]	Erase[1] or destroy[2]	Destroy[3]	Erase[1]	Destroy[3]
READ ONLY CD-ROM DVD-ROM DVD-Video DVD-Audio	Destroy[2]	Destroy[3]	Destroy[2]	Destroy[3]	Destroy[2]	Destroy[3]
RECORDABLE (WORM) CD-R CD-RW	Destroy[2]	Destroy[3]	Destroy[2]	Destroy[3]	Destroy[2]	Destroy[3]

Notes:

1. Erase according to manufacturer instructions
2. Cut into 4 or more pieces, then dispose with non-protectively marked waste.
3. Destroy by disintegration (using a 2mm screen), or incineration, or using a sander to completely remove the recorded surface.

This page intentionally left blank.

HARDWARE SECURITY

This page intentionally left blank.

CHAPTER 5

HARDWARE SECURITY

Introduction

0501. The following additional security measures with regard to the physical security of hardware are to be implemented.

a. **Procurement.** Where possible, orders for IT equipment or spares should conceal its use to process protectively marked information.

b. **Security Records.** Detailed security records are to be maintained of hardware components for all IT systems. It is considered that such records should comprise a file for each system, and contain information which will provide a complete security history of that system.

c. **Recording, Storing and Accounting of Hardware.** All items of hardware that are classed as spares are to be stored and accounted for centrally under secure arrangements. This will help to ensure the integrity of hardware items and help prevent unauthorized modification or tampering. Those items of hardware which contain integral hard disks must be treated as classified equipment, and accounted for in line with the highest protective marking of data stored on the disk.

d. **Registration of Firmware.** Firmware items are to be treated in the same manner as protectively marked documents. The following procedures must be implemented for firmware holding code or data marked SECRET or above:

(1) On receipt or generation, all items of firmware are to be given a unique identifying serial number. This is to be recorded in a MOD Form 102, and is to be indelibly marked on the casing.

(2) When an item of firmware is incorporated into an item of equipment, the temporary disposal section of the MOD Form 102 must be completed, including the serial number of the equipment containing the firmware.

(3) When a firmware item is destroyed, using an approved destruction process, the disposal column in the MOD Form 102 must be completed. Advice on the destruction of firmware should be sought from the DSO through the relevant security staff.

e. **Marking**. In addition to the recording procedures detailed above, terminal screens and/or processor cabinets/boxes should be marked with (non-

removable) labels stating that unauthorized access to the system may constitute a criminal offence under the Computer Misuse Act (1990). Such labels may be obtained through normal publication outlets.

0502. **Anti-tampering.** Nearly all IT hardware can be compromised by forceable attack. Suitable physical protective counter measures must be available and documented in the SPD. It is also possible to mount a surreptitious physical attack by such measures as exchanging components such as chips or inserting bugs. Supervision of maintenance personnel on particularly sensitive systems is important in this respect. In certain circumstances it will be necessary to employ anti-tampering seals for protecting access to components. Currently no security approved anti-tampering seal is generally available so that no great trust can be placed in such items. Where they are employed, they should be referred to in the SPD and SyOPs should set out inspection frequency and action to be taken if there is evidence of tampering.

Physical Security

0503. Physical security measures are to be commensurate with the highest protective marking of data to be processed or stored within the system and the stipulated Mode of Secure Operation.

0504. Minimum security standards of protection are laid down in **Volume 1**. Where cryptographic facilities are required, additional physical security measures may be required and advice should be sought through the security chain of command. All CIS containing official information are subject to protective security surveys and inspections by security units under the direction of security staffs.

Site Selection

0505. Site selection for CIS can have a considerable effect on the protective measures necessary and consequent costs. The CIDA must be involved in the site selection process for ALL systems. The site encompasses not only the location of the system but also the location of spares, system media and support services. There will be a need to identify the following:

a. Highest level of protective marking to be processed.

b. Location of the system.

c. Location of any software and data relevant to the system.

d. Location of spares or back up facilities, if any.

e. Location of any facilities, power supply etc, vital to the functioning of the system.

0506. Once these locations have been identified, physical security controls can be built round them commensurate to the systems Mode of Secure Operation and protective

marking of data processed or stored. Factors to be considered, covering the security of each location both during and outside normal working hours, should include:

a. The structure of the building or offices housing the equipment.

b. The provision of a Secure Room, especially for IT systems with fixed hard disks.

c. The provision of a Security Enhanced Room if the full provisions of a Secure Room are not required. This is a specific countermeasure optimised for CIS equipments not defined within Volume 1, and its details are given at **Annex A**.

d. Doors giving access into the building/offices, and the appropriate locks.

e. Windows that give a view into the building/offices.

f. Containers holding data and/or equipment outside normal working hours. Details of approved secure IT containers are given in other security documentation.

g. Access to facilities which support the system and the protection of these facilities.

h. The requirement for intruder detection systems, their siting, testing and reaction forces.

i. If there is a risk of theft, suitable protective measures are to be taken.

0507. IT systems protectively marked CONFIDENTIAL and above should be so sited that:

a. The TEMPEST risk is minimized, as advised by the CIDA (See **Chapters 2** and **17** for more details).

b. Equipment displaying data cannot be overlooked by unauthorized personnel.

Keys and/or Combination Locks

0508. The requirements for keys and/or combination locks are shown in other security documentation. Additionally there may be non security keys or Personal Identification Devices (PID) to computer terminals/keyboards which should also be afforded the protection commensurate to the protective marking of data processed.

Control of Physical Access

0509. **The Principle.** The requirement of the Mode of Secure Operation and the highest protective marking of the data processed dictate the procedures to be implemented for the control of physical access.

0510. **Security Requirement.** Unauthorized personnel should:

a. Only be permitted essential supervised access and then only in accordance with the need to know principle, security clearance and any other mandatory access regulations.

b. Be prevented from having the opportunity to overlook activity on an IT system.

0511. **Security Measures.** The following measures are to be implemented as necessary:

a. Computer screens should not face access doors or windows.

b. Printers and other output devices should be so located that access can be easily controlled.

c. When terminals are left unattended for any period of time in an unprotected area, the system is to be switched off and any protectively marked media locked away. In certain cases it may be necessary formally to verify that this has been done.

d. Visitors should be clearly identified as such and a log maintained.

e. Uncleared visitors should never be left unattended and are to be escorted as necessary.

Deployment, Storage and Removal of IT Equipment

0512. There is a requirement to detail the procedures for the deployment, storage and removal of equipment.

a. **Deployment.** IT equipment is only to be deployed within a unit on the authority of the Accreditor, who will agree, with the CIDA, the siting and subsequent use. This agreement should be dependent on meeting the requirements laid down within this Chapter.

b. **Storage.** IT equipment, including separated component parts, is to be stored in conditions commensurate with the highest protective marking of the equipment or the information ever processed or stored on the equipment. Care should be taken to ensure that this protection covers information which could still be resident even if overwritten by other data.

c. **Removal.** IT equipment should not be removed from a unit or office without authority of the ITSO, who will consult the CIDA if required. In the event of the removal for maintenance, memory devices are to be cleared of all information as far as practicable. If the equipment still requires security protection then it is only to be passed on to authorized maintenance facilities and worked on by approved service engineers. If removal is for final disposal then advice is to be sought from the security chain of command. Normally it will be necessary to remove or clear all memory devices which may have held information which requires protection. See **Chapter 4**.

Portable IT Systems

0513. For the purposes of this document portable IT systems are defined as those systems for which it is envisaged that there will be no permanent local security environment. This introduces additional risks, particularly of theft and TEMPEST considerations. Such systems, with the appropriate security accreditation, can be used to produce data at any level of protective marking. Within the MOD, portable IT Systems are categorised as follows:

a. Laptops. Laptops, which include most notebooks and palmtops, are Portable IT System equipped with the range of ports normally present on a standard PC.

b. Electronic Personal Organisers. Electronic Personal Organisers include any such devices which are capable of storing magnetic data and exchanging such data with a PC but not equipped with the normal range of PC ports.

c. Electronic Personal Diaries. Electronic Personal Diaries are devices capable of storing data in a magnetic form but which cannot communicate with a PC.

Portables do not include mobile systems such as those mounted on mobile military platforms.

0514. The specific rules which govern the use of portable IT systems are **Chapter 8**. Generic SyOPs for portable systems are at Annex A to Chapter 8.

Data Link Watches

0515. Several manufacturers are now selling watches which can be used to download information from computers using the Windows operating system (desktop PCs portable PCs and some network terminals).

0516. The process involves the loading of specific software onto the above computers which allows data to be converted to what closely resembles a bar code pattern, which can be read by the data link watches.

0517. On no account is any of this software to be loaded onto any MOD owned machine or any other machine on which MOD data is to be processed or stored.

Digital Cameras

0518. Digital cameras, both still and video, that are used to import/export digital pictures to/from CIS are subject to the policy listed below:

a. They are to be registered as peripheral devices.

b. They are to be protectively marked according to the level of the subject that they have been used to photograph.

c. Cameras that have had images or data transferred to them from a CIS, are to be protectively marked to the highest level of data held on the system if this is higher than the protective marking normally associated with the images taken.

d. Cameras that become a protectively marked item as a result of b. or c. above are to be stored in a container appropriate to the protective marking they attract.

e. No imagery from any camera may be loaded onto an Intranet or Internet page without the express permission of the release authority as detailed at **Chapter 10.**

f. At the end of its useful life the digital camera is to be physically destroyed if it has held protectively marked material. (There is currently no approved method of purging a digital camera's memory.)

g. Further policy relating to video cameras is to be found at **Chapter 20.**

"Laplink" Devices

0519. Devices, such as LapLink or PsiWin, which are used to link a portable or desktop system to another portable or desktop systems by the use of software in the transmitting and receiving systems and a physical link, are only to be used with the express permission of the accreditors of each system to be linked. It should be noted that any systems which are to be linked in this manner cannot be regarded as standalone but must be viewed as a network and therefore an SPD must be provided.

Fixed Disk Storage Devices

0520. Special precautions must be taken when fixed disk storage equipment is serviced, repaired or disposed of.

0521. In the case of hired or leased equipment, where protectively marked data is processed, some special agreement is necessary for the retention of disks upon return of the equipment.

0522. If the use of a fixed disk system for the storage of information graded CONFIDENTIAL or above is unavoidable, then the following action is to be taken. When not in use, the device is to be disconnected and stored in an appropriate security container, taking into account the protective marking of the data stored and security position of the environment concerned. NB. Some small systems can be specially modified so that the fixed disk unit becomes free standing, and can be disconnected from the computer to facilitate storage in a standard security container. Either:

a. The equipment must be operated within an approved secure electronic cabinet, either purpose built or of standard design. The PSyA or DSSO Accreditor must be consulted prior to the procurement of purpose built security cabinets.

b. The equipment must be sited in a secure room of the appropriate standard.

0523. If fixed disk equipment is to be removed off-site for maintenance or repair, then one of the following courses of action is to be adopted:

a. The disk platters must be removed and retained on-site, thus declassifying the remainder of the equipment which can then be removed by the contractor. Following repair, the unit will be fitted with new disk platters by the contractor.

b. If it is not possible to remove the disk platters on-site, then the equipment may be taken to the contractor's premises if accompanied at all times by a cleared member of staff. The member of staff is to supervise the complete repair and return of the equipment, or the removal and return of the disk platters for destruction.

c. The fixed disk unit may be released as a classified item to a contractor with the appropriate security clearance. The unit for repair must either be escorted or transported through the Courier Service. The Security Staff must be consulted in such instances.

0524. Depending on the protective marking and sensitivity of data held in the unit and the cost of a replacement unit, destruction may be the only secure and cost effective solution.

Destruction of Hard Disk Units

0525. JSP 440 Volume 1 Chapter 5 Section XVI gives general details of the approved destruction methods for magnetic media, this paragraph gives specific details of

additional methods of destroying hard disk units. Once the unit has been dismantled, the disk unit platters may be destroyed by one of the following methods:

a. By immersion in an acid bath until the magnetic layer of the disk surface has been completely erased.

b. By cutting or breaking the disk into small pieces, followed by incineration or disintegration.

c. By removing the magnetic layer of the disk with emery paper, an emery wheel or disk sander.

0526. There are a number of approved commercial facilities which provide destruction services for magnetic media protectively marked up to and including TOP SECRET. PSyA should be consulted for details of these facilities.

0527. Guidance on maintenance, repair, disposal or return of hardware is shown at **Annex B**.

Disposal of TEMPEST Protected Equipment

0528. In cases where there is a need to dispose of TEMPEST protected IT equipment the advice of the PSyA is to be obtained.

Remote Diagnostics

0529. A number of computer manufacturers have remote diagnostic facilities which can be used to speed maintenance and reduce the time a system is unserviceable. Remote diagnostics are considered to be a security risk and approval must be obtained from the accreditor before they are installed. Where dispensation is granted for the use of dial-up lines or remote diagnostic facilities to access an IT system, the security instructions relating to such a facility must be adhered to. Remote diagnostics are not permitted on protectively marked systems without the express authority of the PSyA or DSSO Accreditor.

ANNEX A TO

CHAPTER 5

SECURITY ENHANCED ROOM

1. For most assessments of physical security, the Physical Security Assessment Matrix within **Volume 1** provides adequate guidance. However, for CIS systems, a simple set of Baseline measures is required where a basic level of physical protection is required, as the following replacement text for what used to be referred to as a "Position 3 environment" has been found less than user friendly by both MOD organisations and their Contractors :

> "a minimum of 6 points aggregated from the Guard/IDS/Entry Control sections of the assessment matrix in Volume 1"

2. The main use of the SER is envisaged to be for :

a. Protection of CIS or related equipments which require to be left in "unattended operations" mode, typically LAN servers and UNIX systems which for reliability reasons are left running permanently, or Facisimile systems requiring 24 hour reception in unmanned areas;

b. Protection of elements of communications equipments that would afford access beyond that available to system users ;

c. Protection of IT equipments with fixed RESTRICTED media ;

d. Protection of UNCLASSIFIED but "valuable and attractive" equipments such as BRENT without STKs ;

e. Other scenarios where a "locked room" has been requested, to provide additional granularity of control of access to a Local Security Environment (LSE) within an already protected Global Security Environment (GSE).

3. **Principle** In most cases, at this level of protection, it will not be possible to physically prevent a determined attempt from entering the space, but the object is to both maximise the difficult of such attempts, and to aid detectability, predicated upon providing a level of protection appropriate for open storage of RESTRICTED information.

4. **Assertions** Any part of the room concerned should be comparable and compatible in strength with the building structure involved: it is futile fitting strong

doors and frames to a room with lightly protected windows, or into a structure offering little protection to forcible attack. Windows can seldom be considered to be security barriers, so actions are required to ensure that attempts at ingress are slowed in order to maximise the chances of observation.

5. It is therefore assumed that the structure into which it is to be built will be of reasonable standard, commensurate with the GSE in which it is installed :

a. A "Protected GSE", where there either is a complete perimeter and guarded or barriered access or frequent external patrols ;

b. Other GSEs will count as "Unprotected"

6. The basic standard of structures will normally be considered to be :

	Protected GSE	**Unprotected GSE**
General	It is assumed that all structures are properly maintained	
External Walls	Minimum 100mm block or brick. Any walls of lesser status can be reinforced by covering openings or "weak walls" with XPM or 10mm plywood	Double-skinned walls would normally be expected. 100mm block or brick can be augmented with an internal layer of XPM or 10mm plywood
Internal walls	Rigid, fixed, construction : movable, "modular" walling is particularly inappropriate	Solid walls would normally be expected. Any walls of lesser status can be reinforced by covering openings or "weak walls" with XPM or 10mm plywood
Floors **Ceilings**	Unless of solid construction, and especially in the case of a drop-ceilings / raised-floors, the boundary for assessment becomes the sides (e.g. walls) and top (e.g. roof or floor) of the void, to ensure that no access to the room via the void is possible	
Doors	Doors providing barrier from GSE to LSE should be of solid construction, mounted on sturdy hinges in frames of rigid construction, with deadlocks to BS3621.	Doors providing barrier from GSE to LSE should be at minimum 44mm solid construction, mounted on sturdy hinges in frames of rigid construction with hinge ("dog") bolts and deadlocks to BS3621.
External Windows	Any windows externally accessible directly or indirectly from ground level that are not double glazed units or fitted with toughened safety glass should at minimum be fitted with 100 micron (0.004") Anti Shatter Film (ASF) to BS6204, and all external opening lights should be fitted with key operated window locks, or secured shut.	
Other Openings	Any external openings (e.g. Grilles) should be firmly secured to the structure of the building, with fixings only internally accessible.	

7. If the structure fails to meet any of the above criteria, then either an approved container to SEAP standard 1200 or Loss Prevention Standard 1228 should be used to store the equipment, or more detailed advice to using the assessment techniques laid down in **Volume 1** will be required, and the physical security adviser should be contacted to discuss the options (e.g. BS4737 Burglar Alarms or Intruder Detection Systems (IDS)) available.

8. In terms of procedural controls, it is assumed that :

a. There is control of visitors to the MOD space during working hours, and it is secured outside working hours, with no "30 minute rule" being permitted during working hours if the space is accessible to unescorted non-MOD personnel ;

b. After MOD working hours, the space is only accessible to approved guard patrols, or, subject to the agreement of the Security Authority, to staff of Other Government Departments (OGD) / List X contractors, if the site/building is shared exclusively with such organisations ;

c. All security keys are held under secure conditions, such as a key safe.

9. Provided that the above requirements are met, then in order to achieve the "Security Enhanced Room" within the structure (remembering this does **NOT** make it a "secure room"), the following specific countermeasures should be implemented, where they do not already exist.

10. **Walls** Any joints in partition walling should be taped to aid detection.

11. **Floors and Ceilings** Any openings (e.g. trap doors), should be either lockable (e.g. with hasp / staple / approved padlock) or sealed closed.

12. **Doors** All room doors should be of 44mm solid construction (fire pattern), without externally adjustable hinges.

13. All room doors in use should be fitted with a Category "C" Deadlock (e.g. Ingersoll SC71) or equivalent, in addition to any Privacy Locks used during working hours.

14. Any Emergency doors in the room should be to fire pattern, and fitted with an Ingersoll Rim Automatic Deadlock (fire pattern), or other approved emergency exit device (e.g. Frazer Bar).

15. Any room doors not in use should be permanently sealed, or kept locked and bolted from the inside.

16. Any glazed apertures of maximum dimension less than 150mm should be fitted with wired safety glass or 100 micron (0.004") Anti Shatter film,

17. Any glazed apertures of maximum dimension greater than 150mm should be fitted with either an internal XPM screen or blanked off, either construction to the standard of the adjoining wall, or by the provision of a 10mm plywood skin.

18. **Windows** Any external windows should at minimum be fitted with 100 micron (0.004") Anti Shatter Film (ASF) to BS6204 (which acts as both a deterrent to ingress, and affords limited IED protection), and those that are not double glazed units or fitted with toughened safety glass should have this ASF applied to both sides.

19. All external opening lights should be fitted with key operated window locks to BS3621, or secured shut.

20. The use of internal XPM screen may be preferred in some cases on external windows, but in such cases advice should be sought from the Security Authority, as it may have deleterious effects, by drawing unwanted attention to the space

21. Any opening lights on internal windows should be fitted with key operated window locks, or secured shut.

22. **Building Services** Any Air Handling Plant or Grilles should be firmly secured to the structure of the building, with fixings only internally accessible.

23. Provisions must be made for external inspection of the room whilst unattended:

a. Wide angle viewers should be fitted to doors : as an alternative, doors with glazed apertures of maximum dimension less than 150mm may be fitted with wired safety glass

b. If the are any spaces hidden from the door viewer, convex mirrors should be fitted to allow their inspection

c. The lighting should either be left on permanently, or an external switch provided so that the area lighting can be controlled for viewing

d. Where buildings are internally patrolled during silent hours, the guard forces must be made aware of the inspection requirement and procedures.

24. This specification will be updated once the provisional European standard for construction and testing of external doors and windows for burglar resistance (ENV 1627-1E) has been ratified.

ANNEX B TO

CHAPTER 5

MAINTENANCE, REPAIR AND DISPOSAL OF IT HARDWARE

1. Under certain conditions of storage and handling, which can arise during the normal lifetime of magnetic storage media, it is possible for a permanent physical image of recorded information to be formed. Once formed, the image remains unaffected by subsequent overwriting or erasure and the information can, in certain circumstances, be recovered using specialist equipment. The circumstances giving rise to the permanent retention of information are not at present well understood, and it is therefore necessary to err on the side of caution. Media with coated surfaces (disks, drums and tapes) present the greatest risk. Backing stores which hold permanent files for long periods are more likely to retain permanent images than those areas of magnetic storage media which are used for temporary storage during processing.

2. The System Manager or deputy are to be consulted if there is a need to release protectively marked storage media to a manufacturer, or contractor, for repair outside the secure perimeter. Advice should be sought from the PSyA as to the guidelines to be followed in these circumstances.

3. Protectively marked storage media which have reached the end of their useful lives are to be disposed of as protectively marked waste in accordance with the instructions contained in this document. (See Annex C to Chapter 4 for the exceptions to this rule.)

4. Protectively marked storage media which have not reached the end of their useful lives but which are no longer required, may be transferred to other secure installations with the agreement of the PSyA. However, in these circumstances, the magnetic storage media is to retain the highest protective marking of information ever stored, and must be protected for that level of protective marking. Prior to removal to another installation, the disks are to be overwritten. (See Annex C to Chapter 4 for more details.)

5. The following procedures are to be implemented for the maintenance of hardware items containing protectively marked information:

a. The System Manager should check that all civilian engineering contract personnel maintaining or repairing items of system hardware processing protectively marked information are appropriately cleared. A list of such personnel is to be maintained.

b. All engineers without appropriate clearances, repairing or maintaining hardware items are to be escorted at all times. The escorting personnel should be technically competent.

c. No items of hardware are to be removed from the installation by engineering personnel without authority from the ITSO. All faulty hardware items requiring replacement are to be destroyed under secure arrangements by the ITSO.

d. The introduction of software into a system by engineers to run diagnostic test routines on items of hardware is strictly forbidden unless the software has been inspected and tested to ensure a freedom from computer virus infection. If necessary, a certificate declaring such routines to be free from such unauthorized software is to be produced by the contract company on each visit.

e. The down-loading of data and/or software from an IT system by engineers is strictly forbidden. If such a procedure is necessary, the ITSO, or his/her deputy, is to carry out down-loading procedures. The data and/or software is to be inspected by this person and declared free from protectively marked data. A certificate to this effect is to be maintained on the system security file.

f. The removal of hardcopy output from the system by engineers is strictly forbidden. If hardcopy output is required by an engineer, it is to be produced by the ITSO and inspected for content. A record to this effect is to be maintained.

g. A detailed record of the maintenance and repair of system hardware is to be maintained. This record should include:

(1) Serial Number.

(2) DTG.

(3) Nature of Fault.

(4) Component Part Repaired/Replaced.

(5) Nature of Repair.

(6) Details of Person Effecting Repair.

(7) Disposal of Replaced Components.

SOFTWARE SECURITY

CHAPTER 6

SOFTWARE SECURITY

Introduction

0601. There is a considerable variation in the degree of security provided by system software. Within the limits of a particular configuration, it is necessary to strike a balance between operational and security requirements. With added sophistication, software becomes more costly to produce and makes increasing demands on hardware and personnel resources. It is difficult to make software completely secure against a skilled and determined attack, and software alone cannot be relied upon to provide complete system security.

0602. This chapter covers the generic issues associated with providing software security mechanisms, including the methodologies for assessing the requirements for functionality and assurance of Passwords **(Annex A)** and the system as a whole **(Annex B)**.

Principle

0603. When implementing a software based solution, the principle of **Least Capability (**sometimes referred to as **Least Privilege**) should be adhered to, whereby Users, and Processes / Hardware acting on their behalf, are only afforded access to those functions and data that are essential for the specific Information Storage, Processing and Exchange Requirements that have been identified to meet the business need.

Procurement

0604. Where COTS software is to be procured with Security Enforcing Functions (SEFs), but the Assurance Requirements calculation at **Annex B** does not produce a need for formal system evaluation, then for it is important for all products not formally approved under the various CESG schemes (e.g. ITSEC or CAPS) that an appropriate MOD endorsement of this software's efficacy is obtained.

0605. For items contained within the Security section of the MOD (DCSA) Catalogue, such approval can be assumed, as inclusion of all items is controlled by the Defence Infosec Product Co-ordination Group (DIPCOG), which is Chaired jointly by InfoSy(Tech) and EC(CCII)IOCM/Proj, and includes CESG representatives.

0606. For all other such COTS procurements, Accreditor sanction must be obtained before procurement action is initiated.

0607. It must be noted that MOD endorsement of a product cannot be construed as any absolute guarantee of functionality or assurance, but rather serves as a statement that no significant exploitable vulnerabilities were known at the time of sanction.

Vulnerabilities

0608. The vulnerabilities of software stem from the following factors:

a. Changes to software, resulting from the addition of new facilities or the correction of detected errors, are unavoidable, and may inadvertently weaken the security controls, or cause some to be bypassed.

b. The need for software changes may allow programmers to deliberately or inadvertently induce malfunctions, or organize the bypassing of security controls.

c. Utility programs are often autonomous and, as such, may be capable of circumventing security measures residing in the controlling or application software.

d. Security loopholes may be caused through incomplete system design resulting from a lack of security awareness by system programmers.

e. Some software manufacturers deliberately introduce "trap doors" into controlling system software. This permits access to the system in the event of a total lock-out. These trap door mechanisms can be discovered by skilled staff and used to bypass the system security controls.

f. Only authorized changes to software are permitted. These must be properly tested and cleared before introduction to a system and such changes are to be fully documented.

0609. A proactive management regime is therefore required to ensure that the impact of such software vulnerabilities is minimised, which at the minimum will involve the monitoring of Official and Open Source information on new vulnerabilities, as laid down at **Chapter 2 Annex G**.

0610. Where Evaluated products or systems, as discussed later in this Chapter, are to be used, consideration should be given to the supplier's Flaw Remediation regime. The *Common Methodology for Information Technology Security Evaluation*, Part 2, v1.0 (CEM) provides a Supplement outlining a framework for obtaining assurance of this regime, under of the ALC_FLR family (Flaw remediation).

Mobile Code

0611. Mobile code is the term used to describe a variety of software technologies that a portable between multiple operating environments (e.g. operating systems). The main technologies covered by this description currently are :

a. Java ;

b. Javascript ;

c. ActiveX ;

d. Visual Basic Scripting (VBS) ;

e. Common Gateway Interface (CGI) scripts ;

f. Server Side Includes (SSI) .

0612. The main vulnerability that mobile exposes is a remote means of circumventing security measures residing in the target platform.

0613. MOD policy on the use of mobile code is contained in a Defence Information Assurance Notice (DIAN), rather than within JSP440, as both the National and Departmental policy is under evolution. The use of mobile code on MOD systems must be specifically sanctioned by the Accreditor(s) of the system(s) for which it is proposed.

Software Records

0614. Detailed records are to be maintained of all software held (as per **Chapter 1**) by units. It is considered that such records should comprise part of the file for each system which contains information that provides a complete security history of that system.

Passwords

0615. For most CIS, basic forms of software access control and individual accountability will involve the use of passwords, which are can be subdivided as :

a. **Long-Term Passwords**. Long-term passwords are normally intended to last for weeks or months. They are administratively convenient and are consequently in widespread use. They tend to be suitable for applications where frequent access is made to a system, with users probably working interactively ;

b. **One-Time Passwords**. One-time passwords may to be suitable for use in batch processing installations and for remote job entry working - two

situations in which it is difficult to give adequate protection to long-term passwords.

0616. Passwords are, therefore, normally to be individually owned, rather than owned in common by a group of individuals. A single password is not to be used on two or more systems which process data at different levels of protective marking. In any installation, reliance is not to be placed solely on passwords for authenticating system users. Passwords are to be augmented by other authentication measures or access control devices, such as can be provided by physical, hardware or software means.

0617. **Annex A** details the MOD method of determining the technical requirements for any automated password system, based upon the system's security profile, and provides guidance on selection of user generated passwords where no automated scheme is implemented.

0618. In the interests of Availability, user passwords that cannot be reset by a System Administrator must be recorded and then stored in a container appropriate to the maximum Protective Marking level of information stored, processed or forwarded on the CIS, with sufficient segregation of access to the password (e.g. sealed envelope) to ensure need-to-know, Special Access approvals, and individual accountability is preserved. All System Administrator passwords must be recorded.

0619. **System Administrator Responsibilities**. In order for a password scheme to be properly operated, the System Administrator (SysAdmin), or System Security Officer (SSO) where the 2 roles exist, must follow certain procedures, which are to be included in the Technical Operation and Maintenance Security Instructions (TOMSyI) for the system as defined at **Chapter 3**:

a. **Initial System Passwords**. Many systems come from the vendor with a few standard user identities (UIDs) (e.g. root, Administrator, Guest, SYSTEM, TEST, MASTER, etc.) already enrolled in the system, normally with generic or even null passwords. The SysAdmin/SSO is to change the passwords for all standard UIDs before allowing the general user population to access the system. This can be easily assured if these standard UIDs are initially identified by the system as having "expired" passwords.

b. **Initial (Temporary) Passwords Assignment**. The SysAdmin/ SSO is to be responsible for assigning an initial (temporary) password for each UID. Passwords and UIDs are to be issued only after the SysAdmin/SSO is satisfied that the potential user holds appropriate clearances. They are to be issued only to those who need them to ensure effective functioning of the system and are not to be granted to people solely on account of their rank or job title. When the initial issue of passwords is made centrally, the distribution is, wherever practicable, to be made by direct personal contact between the SysAdmin/SSO and the user.

c. **Password Change Authorization**. Occasionally a user will forget his password or the SysAdmin/SSO may determine that it may have been compromised :

(i) To be able to correct these problems, it is recommended that the SysAdmin/SSO be permitted to change the password of any user by cancelling the old password and generating a new one. This procedure should be regarded as an auditable event.

(ii) The SysAdmin/SSO is to follow the same rules for distributing the new password as apply to initial password. Positive, formal identification of the user by the SysAdmin/SSO is required when a forgotten password is to be replaced.

d. **UID Revalidation**. The SysAdmin/SSO is to institute a procedure for notifying when a UID and password are to be removed from the system (e.g. when an employee leaves the Unit). In addition, all UIDs are to be revalidated periodically and information, such as phone number, updated as necessary.

e. **Redundant UIDs**. The SysAdmin/SSO is to search regularly for redundant UIDs. If a UID is not used for a pre-determined period, this is to be notified to the SysAdmin/SSO.

0620. **ITSO Responsibilities**. In order for a password scheme to be properly operated, the IT Security Officer (ITSO), or System Security Officer (SSO) where the 2 roles exist, must follow certain procedures, which are to be included in the Technical Operation and Maintenance Security Instructions (TOMSyI) for the system as defined at **Chapter 3**:

a. The ITSO/SSO is to ensure that users are formally briefed on the sensitivity of passwords, and on the measures necessary to protect them, when they are first issued with them. Users are to be formally warned against disclosing passwords to other users, even though they may be employed on the same project and hold identical clearances ;

b. ITSO should obtain and protect sealed copies from users of passwords for any and all systems in the same manner as combinations for physical security containers, and ensure that manual changes are made as appropriate.

0621. **User Responsibilities** In order for a password scheme to be secure, the user must follow certain procedures, which are to be included in the User Security Instructions (USyI) for the system as defined at **Chapter 3**:

a. Passwords produced using CESG's password generation packages are intended to be memorable, but it is accepted that some users need to keep a record of their passwords, especially if they use passwords for several systems.

If passwords are written down, they should be protectively marked at a level consistent with the damage that could be caused by their compromise, and protected accordingly.

b. **Security Awareness**. Users are to keep passwords private and to report changes in their user status to the SysAdmin/SSO. If a user detects any misuse of passwords which may lead to a security violation he is to inform the SysAdmin/SSO. Each user is to sign a statement acknowledging these responsibilities.

Biometrics

0622. The use of biometric technologies (e.g. fingerprint recognition) to support Identification and Authentication (ID&A) mechanisms for defence is not currently recommended for most MOD systems. Any interest in the use of such technologies within MOD should be referred to InfoSy(Tech) through the Accreditor for advice before any procurement action is initiated.

Logon Banners

0623. Wherever possible, a "Logon Banner" (e.g. the Registry setting "LegalNoticeCaption" with Windows NT™ or a text file invoked by ".profile" in UNIX) should be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring. The suggested format for the text would be:

"This computer is provided for the processing of HMG Official Information only, and access by unauthorised persons, or use for other purposes, is subject to the provisions of the Computer Misuse Act, and may constitute a criminal offence. It is to be operated in accordance with the Security Operating Procedures (SyOPs) that must be signed by all authorised users before accessing the system, and all activity on the system is liable to monitoring by Security staffs."

Security Enforcement by Software

0624. The Target of Accreditation (TOA) for the the protection required by any CIS will normally include a number of measures (objectives) to be undertaken within the electronic environment. Such security enforcement by software within systems constructed from Commercial Off The Shelf (COTS) components will normally by achieved by either he operating system and/or specialist security software, rather than by COTS or custom applications, as the latter approach tends to be more complex and thus has a higher risk of failure. When assessing such measures, two aspects have to be taken into account:

a. **Functionality**. That is what Security Enforcing Function (SEF) is required (or claimed) ;

b. **Assurance**. That the security measures have been achieved by selective security enforcing functions and mechanisms.

Modes of Secure Operation

0625. CIS can be categorised as operating within one of four distinct modes of operation, known as the Mode of Secure Operation. Such modes have a considerable effect on the nature of security measures that have to be implemented and, partly, to the threats to which the system is vulnerable. In detail they are:

a. **Dedicated Security Mode**. A mode of operation in which all the users of a system are cleared for, need-to-know about and have access to all the data handled by it. Hence, the system does not enforce national security rules or need-to-know and little or no technical security functionality is required. Note: It may be practicable to run a system at different levels of protective marking using a Dedicated Session approach by utilising exchangeable hard discs at the appropriate level, known as Session Processing, as detailed at **Chapter 3 Annex R** ;

b. **System High Security Mode**. A mode of operation in which the users of a system are all cleared for, and have formal access approval for, all the information handled by it, but not all of whom actually need-to-know about all of the data. In this mode of operation Discretionary Access Control (DAC) may be applied ;

c. **Compartmented Security Mode**. A mode of operation in which the users are all cleared for, but do not have formal access approval for, all the data handled by the system; and who only need to have, and are only given, access to some of that data by means of Mandatory Access Controls (MAC) ;

d. **Multi-level Secure (MLS) Mode**. A mode of operation in which a computer system (or network of computer systems) handles data at various protective markings etc, but for which there are users not cleared for all that data and whose access is restricted appropriately. Hence, the system (or network) is relied upon to enforce the national security rules.

Modes of Secure Operation Summary

MODE	CLEARANCE	FORMAL ACCESS APPROVAL	NEED-TO-KNOW
DEDICATED	**ALL**	**ALL**	**ALL**
SYSTEM HIGH	**ALL**	**ALL**	**SOME**
COMPARTMENTED	**ALL**	**SOME**	**SOME**
MLS	**SOME**	**SOME**	**SOME**

Functionality

0626. HMG Infosec Standard No 1, as interpreted for MOD at **Annex B**, gives only the broadest guidance on authentication and access control, stating that all functionality must be specified in the relevant Security Policy Documents (SPD) since the security functionality of systems or components depends on their purpose. Some further functionality requirements accrue from HMG Infosec Standard No 3 for Interconnected systems, as interpreted for MOD at **Chapter 15.** Features which are required are based on the Mode of Operation as follows:

a. Dedicated Systems.

(1) Lists of authorised users must be maintained that are kept up to date.

(2) All users must be positively identified at the start of each processing session

b. Dedicated Systems which are vulnerable to unauthorised access.

(1) Lists of authorised users must be maintained that are kept up to date.

(2) All users must be positively identified at the start of each processing session

c. System High Systems.

(1) Lists of authorised users must be maintained that are kept up to date.

(2) All users must be positively identified at the start of each processing session

(3) All machine password/generation systems must be approved by CESG.

(4) Functionality must be provided to give users the means to protect their own information from other users e. g. Discretionary Access Control (DAC).

d. Compartmented and MLS Systems.

(1) Lists of authorised users must be maintained that are kept up to date.

(2) All users must be positively identified at the start of each processing session

(3) All machine password/generation systems must be approved by CESG.

(4) Functionality must be provided to give users the means to protect their own information from other users e. g. Discretionary Access Control (DAC).

(5) Functionality must be provided to control access to information based on user clearance and the requirements to protect certain information (e.g. security class) by Mandatory Access Control (MAC).

0627. ISO 15408, the *Common Criteria for Information Technology Security Evaluation* (CC) provides for the concept of pre-defined groups of functionality against which Products can be Evaluated, or which can be used as a baseline for System Evaluations. These take the form of Protection Profiles (PP), some of which have evolved from the Functional Classes of the previous European *Information Technology Security Evaluation* Criteria (ITSEC) standards, and like the similar classes from the older US *Trusted Computer System Evaluation Criteria* (TCSEC) also include Assurance requirements.

0628. Although the generic CC PPs can provide a basis for the functionality requirements for secure systems, they are inherently limited by the need to be applicable to the widest possible audience, and as such Products evaluated against these PP may not meet the whole Defence requirement. Similarly, System specific Targets of Evaluation (TOE) may be composed from generic CC PPs, but may well need additions to meet the overall requirement, for instance for CIS primarily used as communication switches or where data integrity is the main concern.

0629. MOD is therefore investigating the possibilities of generating a series of CC Functional Packages (FP) which are smaller elements of functionality that can be used to either build custom or generic PPs for defence orientated products, or as a basis for a TOE for a system evaluation. Unlike PPs, a FP is a free-standing items and not bound to a level of Assurance. The focal point for this activity in MOD is the DIPCOG, and projects finding that generic PPs do not provide either the granularity or functionality they require, or requires the wrong degree of Assurance, should contact InfoSy(Tech), through their Accreditor, for further advice.

0630. A selection of interim FP definitions is given at **Annex C**, based on the generic functionality identified at **Annex B** in respect of systems with a Marginal Assurance Requirement.

Assurance

0631. When developing a new CIS, HMG Infosec Standard No.1, as interpreted for MOD at **Annex B**, is the approved methodology to link the required functionality to an appropriate level of assurance. If a high assurance requirement is derived, this can lead to a significant increase in project costs.

0632. Formal evaluation procedures are required to obtain both Assurance, which is the confidence that may be held in the security provided by the TOE, and Correctness, which refers to the accuracy with which security claims are reflected in this target. The Assurance and Correctness Levels derived for new developments will be in term of the CC, but procedures exist to allow Accreditor recognition of Products or Systems evaluated against the older ITSEC, or even the previous *UK Levels* (UKL), which have all been approved for use by HMG where appropriate. The use of any other assurance method, such as TCSEC, will require consultation with both the Accreditor and the Defence Technical Security Authority, InfoSy(Tech).

0633. Where a requirement for formal assurance is identified, this will need to be supported by Certification in accordance with Government Minimum Standards. Certificates are produced as a result of Evaluations, of systems and products, undertaken by accredited organizations known as Commercial Evaluation Facilities (CLEFs), with the Certification being undertaken by the UK Certification Body (CB), jointly managed by the Communications-Electronics Security Group (CESG) and the Department of Trade and Industry (DTI).

0634. Both CC and the older ITSEC criteria benefit from International Mutual Recognition (MR) Agreements, which permits Products evaluated in one country to be used in the other signatory countries to the MR Agreement. Where MR is not a concern, for instance for systems being built for MOD, or for products whose vendors do not perceive a requirement for formal MR, there are a number of other CESG schemes which may be appropriate for use by defence, using alternative Assurance Packages (AP) to those covered by the MR Evaluation Assurance Levels (EAL). At the time of publication, the alternative CESG APs are :

a. **SYS** A hierarchy, similar to EAL, of assurance levels that can be specified, intended primarily for Government or Critical National Infrastructure (CNI) System Evaluations. SYS evaluations are intended to produce savings in both timescale and costs compared to EAL, but without reducing the overall confidence that that no significant exploitable vulnerabilities have been found by the process. The savings accrue mainly from removal of some of the formality required for MR ;

b. **FTA** The Fast Track Approach (FTA) to product evaluation is intended to produce a rapid assessment of products, either where a full scale evaluation is not practical, or where there is a desire for an initial assessment of a product to allow its introduction to service before formal evaluation completes. Unlike CC or ITSEC evaluations, the Sponsor of a FTA evaluation is a representative of the user community, rather than the vendor, and only Government or CNI may sponsor FTA. For defence, all FTAs must be sponsored through the DIPCOG to ensure that the TOE is appropriate for re-use, but the funding of Defence FTAs will fall normally all to the vendor, or occasionally to the requesting project ;

c. **CHECK** This is a formalised system test methodology jointly operated by CESG and MOD (formerly DERA), providing the functions of both an ESE Verification (EV) and a Vulnerability Analysis (VA) as laid down at **Chapter 12,** utilising either in house resources or approved consultants. CHECK is only appropriate for low assurance requirements, and will normally be regarded as equating approximately to EAL1, and on occasion to EAL2 if so agreed by the Accreditor(s).

0635. Additional APs are also being considered, and in the interim their use for defence will be subject to approval by InfoSy(Tech) until this document is updated. The use of either SYS, FTA or CHECK must be agreed with the Accreditor(s) by procurement authorities in advance, as in many cases the more rigorous approach of formal CC evaluations will be necessary.

0636. All of these evaluation methodologies only apply to the Computer Security (CompuSec) aspects of SEFs, and where Communications Security (ComSec) techniques (i.e. cryptography) are also contained with the TOE, this requires separate approval. The corollary of this is that a ComSec approval does not necessarily mean that all CompuSec aspects of a TOE have been analysed, and procurement authorities must satisfy their Accreditor(s) that both aspect have been comprehensively addressed where both are required.

0637. For defence use, as detailed at **Chapter 23**, all cryptography must be formally approved by the National Technical Authority (NTA), CESG, before being used to provide either ComSec and/or CompuSec for Protectively Marked material. The main way in which this is achieved for commercially produced Baseline Grade (BG) and

Enhanced Grade (EG) items is the CESG Assisted Product Scheme (CAPS), which provides assurance of the cryptographic components of a system and software functionality that directly supports these components.

0638. Where MOD projects engage in any form of Assurance Activity, be it System Evaluations, or sponsoring Product Evaluations, the contract must be let in such a way as to allow MOD re-use the efforts made in such assurance activities as far as possible, to prevent nugatory effort.

0639. Additionally, it is important to maintain a central MOD knowledge base of products known to have been so tested. On completion of such activities a Assurance Activity Feedback Form, as illustrated at **Annex D**, is to be completed and forwarded to the MOD's Infosec technical coherence branch, EC(CCII)IOCM/Proj.

Accounting for Audit Purposes

0636. Once a CIS is in use, it is essential for CIS security management personnel to be able to track the way in which the system is used and to ensure that security controls are effective in practice. Specific events and details relating to the operation of the system and its security controls, must be recorded for subsequent inspection and analysis.

0637. The degree and depth of monitoring and detail recorded for auditing will depend on the highest level of protection required by the data being processed or stored and the Mode of Secure Operation. For dedicated systems none may be required. Additionally the type of system, the location and physical security measures in place, will also influence the degree and depth of the monitoring and audit. Security staff will give advice on the security measures that are to be implemented.

Responsibilities

0638. It is the responsibility of the ITSO or a nominated individual to carry out audits of the accounting records. The frequency is to be laid down in the SyOPs and a record kept of all such activity. Similarly the appointed individual should be identified by post.

Aim

0639. The aim of the accounting and auditing facility is to identify any types of normal or abnormal activity of potential security significance on the system. Anything associated with a user's access to the system or to a protected object (e.g. a file, device, or other computer) within the system, is a security related event.

Recording

0640. This section gives information on the structure of the automatic recording of security relevant events that take place on a system. These events form the accounting

file which provides a basis for the audit trail. They are to include, as a minimum, the events listed below.

0641. Security relevant events fall into two categories, namely legitimate events and violations.

a. The following events shall always be recorded:

(1) All log on attempts whether successful or failed.

(2) Log off (including time out where applicable).

(3) The creation, deletion or alteration of access rights and privileges.

(4) The creation, deletion or alteration of passwords.

(5) The introduction of all software (authorized or unauthorized).

b. The following events may be recorded or may be configurable.

(1) The production of protectively marked hard or soft copy output.

(2) The creation or deletion of files and the assigning of their level of protective marking.

(3) Any re-grading of the level of protective marking either of data objects or log in privileges.

(4) Introduction or removal of storage media.

(5) Backup operations.

(6) Attempts to access data/files and whether successful or not.

(7) Attempts to disseminate data/files and whether successful or not.

(8) The copying of protectively marked data/files within the system.

0642. For each of the events listed above, the following information is to be recorded:

a. Type of event,

b. User ID,

c. Date & Time

d. Device ID

0643. The accounting records should have a facility to provide the System Manager with a hard copy of all or selected activity. There should also be a facility for the records to be printed in an easily readable form.

0644. All security records are to be inaccessible to users without a need to know.

0645. Operating systems are capable of recording vast amounts of detailed information about a wide range of system events. However, most operating systems have facilities to allow the system manager to define and select which events are to be recorded in the audit log as security audit messages. Generally, for the purposes of system security, it is the recording of exceptional events that is required and will be of greatest interest in determining compliance with the SSP.

0646. **Unattended Terminals.** Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, to prevent an attacked making use of an unattended terminal. An audit report is to be created of the system-generated logoff, so that repeated incidents may be dealt with by the SSO. For installations employing very high security measures, it may be thought necessary to enforce a re-authentication procedure at frequent intervals (say 50% of the forced logoff time) during the session.

0647. In order to assist with technical inspections and recovery from system failures etc a record is to be maintained of all software fixes and patches that are made to a system.

0648. Collecting security audit messages in the security audit log file is useless without periodically reviewing it for suspicious activity. Most operating systems have facilities for generating reports from the audit log. Utilities are also generally provided to analyze the log for patterns of unusual behaviour. The analysis over a period of time may reveal a pattern of activity that clearly indicates security violations. Particular attention should be taken with accounts which have enhanced privileges.

Baseline Patterns

0649. It is important to establish what are the normal and acceptable patterns of use of a system before potential security problems can be recognised. Once this is done procedures should be established to regularly review the audit log. Normal events can be identified by answers to the following:

a. What are the typical hours most users work?

b. Who are the specific users who normally operate with higher privileges?

c. Which programs generate system security events as part of other applications?

d. What are the regular batch or network jobs that run at specific times of the day?

0650. The size, number of users and amount of system use will help determine how often this should be done. The most common type of report is a brief daily listing of selected events that is created from running a batch job every evening before midnight. It is important that such reports are reviewed as soon as possible in order to gain early warning of any system security breaches. Analysis of audit logs is a specialised job and requires considerable experience and expertise to recognise events of suspicious activity requiring further investigation and follow up. Logs must be protected from unauthorised modification.

Suspicious Activity

0651. Whenever this analysis reveals a potential security incident a detailed investigation of the relevant security events should be carried out. Common forms of system attack that should be recognised as suspicious include:

a. Hunting for access lines;

b. Hunting for passwords;

c. Attempting break-in;

d. Changing or creating user authorizations;

e. Granting or stealing extra privileges;

f. Using a node as a gateway to other nodes;

g. Using network configuration interrogation tools.

Retention of Security Record

0652. In accordance with national guidelines all recordings which refer to data protectively marked SECRET or higher must be retained for a minimum of 2 years. Recordings of data protectively marked CONFIDENTIAL and below should be retained for a period, of not less than 6 months, to be decided by the system accreditor.

Intruder Detection Systems

0653. MOD policy on the use of Intruder Detection Systems (IDS), and related Real Time Monitoring (RTM) technologies has not yet been finalised, but the following

initial guidance and policy framework can be given. Before attempting to deploy any IDS or RTM capability within MOD, InfoSy(Tech), JSyCC, and EC(CCII)IOCM/Proj should be consulted through the Accreditor(s) for current guidance.

0654. The term Intrusion is defined in **Chapter 11**, as one of the likely outcomes of RTM or IDS detecting an occurrence with be the need to handle an incident. At the simplest, the review of accounting records by security staffs can be considered to be a special, manual, case of IDS.

0655. IDS is a means of detecting unauthorised use of, or attack upon, a computer or network. The use of IDS is not a panacea, it is only one of a number of measures which may be required to protect a system or network. It should be noted that in order for an IDS to work, a number of supporting factors will need to be considered:

a. Where the IDS is used to analyse data from more than one Host or Probe, it is essential that synchronisation of timebases is provided if the resultant analysis is to be of any value. For evidential purposes, it is recommended that the master timebase be synchronised to a source at least as accurate as a "Stratum 2" Internet time service. To conform with other operational practice it is recommended that ZULU time be used for all IDS recording and reporting;

b. Any system components holding information to be used by the IDS will need to have their mass storage capacity aligned to the volumes generated between analysis periods, particularly if content-based rather than event-based logging is deployed ;

c. An IDS may cause inadvertent Denial of Service (DoS) by "flooding" any shared communications bearer, and this should be considered in system sizing.

0656. A Risk Assessment approach will be required to determine the nature of the IDS to be provided, both in terms of Functionality and Assurance, in accordance with the requirements laid down at **Chapter 6 Annex B** and at **Chapter 14**.

0657. The protection service required may vary depending on the IDS employed. Where Confidentiality is the main concern, the risk assessment will be driven by Protective Marking, but where Integrity and Availability services are the main driver, Asset Valuation in terms of Criticality Level (CL) should primarily be used to drive the Risk Assessment.

0658. IDS is either Host based (HIDS) or Network based (NIDS). A mixture of each type offers the most effective defence. The type and location of IDS will depend on the level of threat and the functionality required.

0659. Currently, IDS offers maximum protection when incorporated within the Secure Managed Interface (SMI) at the entry/exit point(s) of a system or network, either as an

element of a Boundary Protection Device (BPD) or as a standalone BPD in its own right.

0660. Critical hosts within a network (such as servers) should also be protected with additional host based IDS, which may be implemented as software Agents on hosts, or as additional, free-standing Sensors. In such cases the IDS may be configured not only to detect intrusions, but also to provide some internal anomalous behaviour detection.

0661. An IDS can use either Event or Content based Logging, with the latter approach having significant performance and sizing implications.

0662. The self-protection requirements for the IDS platform and/or any cryptography used within any IDS should be assessed on the same basis as the Identification and Authentication (ID&A) barrier(s) for the hosts being protected, as laid down at **Annex B**. It may be necessary to provide a dedicated infrastructure for IDS reporting, separate from that being monitored by the IDS itself.

0663. It is the intention of MOD to use a mix of IDS products which are compatible and interoperable. Although standards for recording of information such as US Department of Defense (DOD) Common Intruder Detection Framework (CIDF), and the Internet Engineering Task Force's (IETF) Intruder Detection Exchange Format (IDMEF) and Incident Object Description and Exchange Format (IODEF) have been proposed, most current commercial products are, however, proprietary, and do not conform to these standards. Investment in IDS may therefore require a change to a standards conformant product at some future time, if the IDS is to be integrated into a MOD-wide IDS structure, but as an interim measure an ability to produce "syslog" format if required is highly desirable.

0664. It is strongly recommended that all IDS installations are implemented so as to make their output accessible to a recognised MOD Monitoring and Reporting Centre (MRC), as defined at **Chapter 11**, in addition to any local monitoring. In the case of IDS provided for Criticality Level (CL) 1 and 2 MOD CIS, the provision of a feed to a MOD MRC is mandatory, and this MRC must be operated for at least the same period as the subject CIS.

0665. CESG's Interim Guidance on Protective Monitoring is reproduced at **Annex E**.

This page is intentionally left blank

ANNEX A TO

CHAPTER 6

PASSWORDS

Password Schemes

1. **Minimum Standards.** Minimum standards for passwords, derived from standards published by the National Technical Authority (NTA), CESG, are as follows :

a) Where required, all machine password generators and encryption algorithms must be approved by CESG, where approvals will either be COTS/GOTS products as endorsed by the CESG Assisted Product Scheme (CAPS), or specific approvals for system implementations as approved by CESG X11;

b) Users are to be able to change their own passwords ;

c) To assure accountability, the capability is to exist for the System Operating Authority (SOA) to access and evaluate accountability information (e.g. date, time, and terminal of last login), by a secure means, within a reasonable amount of time and without undue difficulty ;

d) If an incorrect identifier/password is entered, the terminal or network address should be disabled for at least 5 seconds. If 3 consecutive incorrect attempts are made the disabling should be for at least 5 minutes. Two further incorrect attempts should result in "lock-out" until reinstated by a system manager. If lock-out is not technically or operationally feasible the password size must be increased in length by 2 characters. Incorrect attempts should be logged and audited to detect systematic attempts at penetration ;

e) Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, to prevent an attacker making use of an unattended terminal ;

f) The Strength of Mechanism (SoM) for password shall be chosen :

Level	Format	Change	Generation	Encryption	Sharing
EAL 6 & 7	12 filtered "Clearview" characters Use of tokens desirable	Monthly	CESG supplied algorithm, seeded from change time	CESG supplied algorithm including cryptographic checksum and change time	No sharing permitted
EAL 5	9 filtered "Clearview" characters Use of tokens desirable	3 monthly	CESG supplied algorithm	CESG supplied algorithm including cryptographic checksum	Between maximum of 2 systems at same protective marking
EAL 4	6 filtered "Clearview" characters and 2 randomly chosen digits	6 monthly	CESG supplied algorithm, or CESG generated passwords	CESG supplied algorithm	Between multiple systems at same protective marking
EAL 3	6 filtered "Clearview" characters, or 4 digits if tokens are also used	9 monthly	CESG approved algorithm or central generation	CESG approved algorithm. On small systems (i.e. those with fewer than 11 users) password file access controls may be used instead	
EAL 2		12 monthly	Machine generation is desirable but not mandatory. If no generation, passwords should be retained in the history file and not re-issued space.		Between multiple systems provided all authorised users are cleared for access to all systems
EAL 1 (and other cases needing Access control)	4 digit numbers				

2. **Login to a Connected System**. Some form of trusted identification forwarding is to be used between hosts when users are connected to other system through a network. When trusted identification forwarding is not used, remote hosts are to require that the

user authenticate himself, by supplying his UID and password. The password for use on a remote host is to be different form that used on the local host.

3. **Transmission over a Communications Link**. When passwords require to be transmitted over a communication link, from one part of a computer system to another, they are to be protected by a means appropriate to their protective marking.

a. **Passive Wiretapping**. Communication lines between terminals and computers are to be adequately protected (see **Chapter 22 -24**).

b. **Active Wiretapping/spoofing**. Spoofing occurs when a system is fooled into believing one user is at the terminal when another user is actually there. Computer systems can be easily spoofed.

c. These threats can be prevented by encrypting all communication between the terminal and the computer. Passwords are not to be used as encryption keys, or as part of encryption keys.

4. **System Breakdowns**. In the event of a system breakdown, special operating procedures may be needed to ensure a quick and secure restart. There are serious dangers in allowing password files to be restored by standard mechanisms, such as retrieval of a previously valid version for archives. One-time passwords are particularly vulnerable to this approach, since they may receive a second lease of life.

5. **Notification to the User**.

a. Upon successful login, the user is to be notified of:

(1) The date and time of user's last login (or logoff).

(2) The location of the terminal used for the last login.

(3) Each unsuccessful login attempt to use this ID since the last successful login.

(4) Action to be taken if this information is not accurate.

b. This provides a means for the user to determine if someone else is using, or attempting to guess, his UID and password. Such notification is to be given immediately after successful login; the system is to require an acknowledgement from the user (a key depression) that the information has been read before the screen is overwritten with the next set of broadcast information.

c. If the login is unsuccessful, a simple error message is to be generated which is to be detailed enough to be of help to a genuine user, but not so explicit

as to assist an attacker. Any error messages are to appear at the end of the attempted login, regardless of where in the procedure the error occurred.

Technical Measures

6. The following technical requirement should be included in the Security Target (ST), as laid down at **Chapter 3**, for any system where a password generation or encryption technology is to be implemented, other than where this functionality is already pre-approved as part of a CESG Evaluation. This represents the generic Protection Requirement for Software Cryptographic Modules for System High processing in protected environment:

a. A cryptographic module shall employ either role–based authentication mechanisms or identity–based mechanisms in order to verify the authorization of the operator to assume the desired role(s) and request the desired service(s)

b. If the enclosure includes any doors or removable covers, then they shall be locked with pick–resistant mechanical locks that employ physical or logical keys, or they shall be protected via tamper evident seals (e.g. evidence tape, holographic seals)

c. Documentation shall include a detailed description of the software design within the module, with a detailed tracing of correspondence between the design and the cryptographic module security policy. A complete source code listing shall be provided, with comments that clearly depict the relationship of each software element to the design.

d. Cryptographic software shall be installed only as executable code, in order to discourage scrutiny and modification by users

e. Cryptographic algorithms and mechanisms must be approved by CESG

f. All cryptographic software, key variables (KV) and other critical security parameters shall be under the control of an operating systems that provides controlled access protection (i.e protection to ITSEC F–C2, certified to an assurance level appropriate for the system)

g. The discretionary access control mechanisms provided by the operating system shall be employed to protect all plaintext data, cryptographic software, KVs, authentication data, and other critical security parameters from unauthorised access, as per the following requirements:

i. The operating systems shall provide the capability to specify the rights (execute, write, delete) of operators to cryptographic program images and data contained on the cryptographic module's secondary store or in computer memory

ii.The operating systems shall provide the capability to prevent all operators and non operating system (i.e. all operator initiated) executing process from modifying cryptographic processes

iii.The operating systems shall provide the capability to specify a separate set of operators and cryptographic processes for each of the cryptographic module software components (KV, critical security data, plaintext), both on secondary store and in memory, such that only elements within a component's set can read entities within that component

iv.The operating system shall provide the capability to specify a set of operators who are authorized to enter cryptographic keys and other critical security parameters

h. KV entry and output may as plaintext if manually entered, but encrypted if electronically distributed

7. For other modes of processing, or operation in unprotected environments, advice should be sought from DSy(Pol).

User Generated Passwords

8. Where it is not technically possible or required to implement CESG approved password generation mechanisms, the following guidance should be followed to ensure that a password of reasonable strength is selected.

a. Passwords should not be a dictionary word or any proper name ;

b. Passwords should not bear any direct or indirect relationship to the User (e.g. own, family, pets' or location names or nicknames, car registration numbers etc.) or Post (e.g. job tally, project name) ;

c. Passwords should be at minimum 6 characters long – 9 characters is preferred ;

d. Password should normally include numeric and "special" characters (if so permitted by the system) as well as alphabetic characters.

9. One method of producing difficult to attack passwords that can be relatively easily remembered (or recreated) is to use the Pass Phrase technique :

a. Select a 3 or 4 word phrase (e.g. Main Building London or Defence Ministry Head Office) which, unlike the examples, should not bear and obvious relationship to the user or post ;

b. Take first 3 characters of each of a 3 word phrase (mai bui lon), or the first 2 of a 4 word phrase (de mi he of) ;

c. Substitute "lookalike" characters where possible (e.g. 0 for o, 1 for i, 5 for s), resulting in the passwords of 'ma1bu1l0n' or 'dem1he0f'

10. If the system concerned treats upper and lower case characters as being different for password purposes, this can be further strengthened by alternating upper and lower case in the password (e.g. ('Ma1Bu1L0n' or 'DeM1hE0f')

ANNEX B TO

CHAPTER 6

MOD ASSURANCE REQUIRMENTS FOR COMMUNICATIONS AND INFORMATION SYSTEMS

(From HMG Infosec Standard No. 1
"Assurance Requirements for IT Systems")

Background

1. Rapid and unremitting change in the IT world means that fixed and absolute security solutions are hard to define and harder to achieve, so the process of risk management calls for a healthy measure of pragmatism. The method documented here has evolved over nearly a decade, as a combination of widely-accepted basic principles and actual experience within HMG, and this document helps security staff decide what level of technical security is appropriate to achieve their overall risk management aim.

2. A balanced set of Security Measures will invariably include elements of physical, personnel and procedural security, as documented elsewhere in the Manual. These may be extant, planned or purely hypothetical, but values for the various parameters used for the calculations described later in this document have to be defined, as it is these that dictate the extent to which technical security will be relied upon. The decision is arrived at in a way that highlights the trade-offs between one form of protection and another to strike the optimum balance.

3. Technical Information Security (InfoSec) Measures may include elements of Computer Security (CompuSec), Communications Security (ComSec) and Radiation Security (RadSec). Although all of these issues need to be considered, this document deals primarily with CompuSec Measures, that is, specific security functions, such as verifying passwords, implemented in hardware or software.

4. It is necessary to determine both the functionality of such a Security Measure, that is, what it does, and how much reliance can be placed on its robustness, expressed as an Assurance Level. This CompuSec Target of Accreditation (TOA) may entail a formal Evaluation of the system by a Commercial Evaluation Facility (CLEF), or it may be sufficient that the system incorporates products that have been formally evaluated by a CLEF and Certified by the UK Scheme to the required Assurance Level, as derived from this document.

5. The CompuSec principle which can be stated as 'every specific Threat should be countered or the Risk posed by that Threat deemed acceptable', will indicate to a great extent what functionality is needed.

Status

6. It is a Baseline requirement that those responsible for securing protectively marked information within HMG will use this agreed standard method, which has been specifically tailored to the current security environment. 'Baseline' in this context means that it is expected that the document will be applied in all cases, unless there are strong, documented, reasons for not doing so.

7. This document has been derived from the generic HMG Infosec Standard, but has been adapted in line with Departmental Security Officer's (DSO) Discretion to make it more applicable to MOD's various operating environments. It is therefore the MOD Minimum Standard, and any comments regarding it should be directed to the InfoSy(Tech) office in DDefSy.

Applicability

8. Where specially sensitive classes of information are stored, processed, or forwarded, the MOD is bound to comply with the regulations governing their protection either in the terms of a bilateral / multilateral agreement (typically for multinational instances) or as a condition of release (for externally owned material).

9. The main instances of this will be for STRAP material, as regulated by **Volume 5**. For STRAP and other especially sensitive material, in addition to carrying out an assessment against this document, an assessment against the compartment(s) requirements must also be carried out, and the **higher** of the requirements will form the baseline. In cases where this cannot be met, InfoSy(Tech) and the Compartment Infosec Representative(s) (CIR) should be informed in writing before proceeding.

Scope And Limitations

10. This document is primarily intended to address the risk of compromise to official IT systems carrying protectively marked data. While it recognises that compromise may arise from accidental as well as malicious causes, it does not cover safety-critical requirements. Such requirements are addressed by appropriate industry standards and regulatory authorities. For the purposes of this document software should be considered safety-critical if its failure would result directly in a hazardous situation. If, however, software failure or compromise would open up a way for a Potential Attacker to create a hazardous situation then it may be considered as security related as well as safety-critical, and this document can apply.

11. The method applies primarily to individual Security Barriers, and analysis of a complete system can require a large number of very similar calculations (use of the software tool will ease this task).

12. The method can also apply to a group of Security Barriers, or even a 'monolithic' approach for the whole system as was common with previous issues of this method, generating only one Assurance Level, although this may result in an Assurance Level higher than necessary for some or all of the Security Measures. This may be appropriate when:

a. A solution based on a single "Commercial-off-the-shelf" (COTS) or "Government-off-the-shelf"(GOTS) product is envisaged ;

b. Users and data are particularly homogeneous.

13. However, it may be advantageous to implement some parts of the system to a higher degree of Assurance than others, and segregate the more sensitive operations in those parts. At the cost of multiple assurance calculations for the different aspects, it may be possible to justify lower Assurance Levels in some parts of the system.

Principles For Use

14. This methodology should be used at the design stage to investigate various design and configuration options, including changes to the Physical, Personnel or Procedural Security Measures, to arrive at an optimally cost-effective solution.

15. Having carried out a preliminary assessment based upon an outline solution, the calculated assurance level(s) will fall within one of 5 defined CompuSec TOA groupings which indicate the assurance approach required. In all cases where Evaluation, Verification, or Analysis is advocated, the goal is to prove that "no significant exploitable vulnerability exists".

16. If the assurance approach indicated by the indicated TOA group is not felt to be feasible, the Accreditor should in the first instance consider whether either of the following approaches should be applied :

a. Enhance or alter other Security Measures to reduce the calculated Assurance Levels to those to those which are more easily achievable (or in some cases, no evaluation is necessary) ;

b. Decide the risk is unacceptable, and do not proceed.

17. Should this approach still not produce an acceptable solution, a risk management decision will be required, and the Accreditor will therefore need to produce a risk assessment for the appropriate Senior Responsible Officer (SRO), as laid down at

Chapter 2. The Accreditor should therefore consult InfoSy(Tech) for an individual assessment as to which of the following courses of action - approximately in decreasing order of preference – is likely to produce the lowest residual risk :

a. Incorporate Certified products as included in the Assured Products List (UKSP 06), certified to the level indicated by the calculation, into the system and perform a System Evaluation to a lower level than the calculation indicates, and accept the additional risk ;

b. Arrange for the system to be Evaluated and Certified under the ITSEC, Common Criteria, or other CESG recognised schemes to a level lower than that calculated by this method, and accept the additional risk ;

c. Incorporate certified products, as included in the Assured Products List (UKSP 06), certified to the level indicated by the calculation, into the system in appropriate places and have an approved ESE Inspection (EI) and Vulnerability Analysis (VA) by Competent Bodies carried out on the soundness of the configuration and accept the additional risk ;

d. Arrange for an ESE Inspection (EI) and Vulnerability Analysis (VA) by Competent Bodies to be carried out the system, and accept the additional risk ;

e. Do nothing and accept the additional risk.

18. Experience has shown that when several Certified Products are combined in a system, there are increased problems caused by mis-configuration or misuse, and by interactions between products. In such situations a System Evaluation is highly desirable. If only one product provides all the security functionality, mis-configuration or misuse is less likely, and a System Evaluation is not usually necessary.

19. Before proceeding with ESE Inspection (EI) and Vulnerability Analysis (VA), the Accreditors will require evidence of a sensible baseline against which to proceed (analogous to the Target of Evaluation (TOE) used in formal evaluations), which will probably take the form of a System Configuration Model (SCM) that can be validated and checked by the Verification staff. It should be remembered the system's identified Criticality Level (CL) also has an inherent Compliance Requirement for other Verification activity throughout the system lifecyle.

Accreditor Discretion

20. This is a risk management tool, and if the method is followed and the Security Measures Evaluated and Certified to the level indicated then the Residual Risk should be acceptably low.

21. However, even the best Technical Security Barriers cannot alone protect fully against worst case situations, for instance a determined knowledgeable Potential

Attacker with unlimited access to the system. If Accreditors consider that even the very low Residual Risk is unacceptable, they may, in consultation with InfoSy(Tech), wish to exceed the recommended levels of Assurance or add other forms of protection.

22. The calculation works to a precision of one decimal place, with the calculated Assurance Level being rounded to the nearest whole number to give the required Assurance Level. In borderline cases Accreditors may wish to round either way if, in their opinion and for justifiable reasons, they feel that there are local factors which the calculation does not adequately take into account. Examples of such justification would be a very strong security management regime which would allow a reduction in the requirement, whereas a poor history of the prime contractor in delivering compliant security solutions will of course necessitate rounding up. In all such cases the reasoning must be included with the records of the calculations.

Very High Or Very Low Assurance Levels

23. Should the recommended assurance level not be achievable in practice then this means that wholly acceptable technical security for the configuration under consideration is not normally possible with current technology. This is the case where a MOD Special Protection (SP) TOA is indicated.

24. Should the calculation produce an Assurance Level of zero or lower, this means that no formal Certification is needed. However this should not be interpreted as meaning that no security functionality is necessary, and it becomes a MOD Best Current Practice (BCP) Target of Accreditation. It remains up to the Accreditor to take a considered view and decide whether exceptionally the security functionality could be omitted.

Reaccreditation

25. Where system security parameters change, for instance through new network connections, large change in user population or type of data, a fresh assessment using this document is recommended. The Accreditor will be a key player in this review process, and this may require that the system is formally reaccredited.

Concepts

26. **Potential Attackers** A Potential Attacker is anyone who is not an authorised user of the data or system. In some cases people may be Potential Attackers even though they have legitimate access, for instance if they are allowed to see information but not modify it, then they are Potential Attackers as far as an Integrity attack is concerned. The following are examples (in no particular order) of groups of people who may be Potential Attackers:

- system users without the necessary clearance level for the data

- system users without the necessary Special Access Approval
- system users with no need to know the data
- maintenance staff
- cleaners
- journalists
- investigators
- third party contractors
- foreign intelligence services or their agents
- terrorists
- extremists
- competitors

27. Potential Attackers will vary considerably in how likely they are to try to mount an attack, the type of attack, what resources they can bring to bear, how much effort they are prepared to expend, and the opportunity they have to mount an attack.

28. Attacks may or may not be easily detected. A subverted employee would try to remain undetected, whereas a disgruntled employee might try a blatant attack on data Integrity in order to cause embarrassment.

29. Potential Attackers may be extremely knowledgeable about the system they are attacking, or they may know little. The availability of ready-made hacking tools can greatly enhance the effectiveness of an Attacker.

30. As a result of this diversity, the treatment of Potential Attackers in this document is necessarily a simplification. There is an assumption that Checks and Clearances (BC, SC and DV) reduce the chance that a person so cleared will mount an attack, and this applies to attacks on Confidentiality, Integrity and Availability.

31. Potential Attackers' capabilities may be limited by the system itself, either in the facilities the Potential Attacker can bring to bear or because there is limited time for the Potential Attacker to access the system. The total facilities a Potential Attacker has available are not relevant, only those that he can bring to bear on the target of attack.

32. In a networked system, all those with physical or logical access to the network should be considered as Potential Attackers except when they are legitimate users of the data to be protected by the Security Barrier under consideration.

33. Ways of grouping data, Potential Attackers and security functionality are developed below that clarify this idea.

34. An essential feature of the method hinges on the distinction between a Security Measure and a Security Barrier. The former provides protection against some particular aspect of the threat that Potential Attackers pose to the data. The latter is a combination of one or more such Security Measures, which may be independent or co-operating; taken as a whole it provides the total protection required to counter the threat to the data from the group of Potential Attackers.

35. In a monolithic system, the Security Barrier comprises all the security functionality of the system. It is important to bear in mind the distinction between Security Measures and Security Barriers whilst reading this section. The discussion is mainly in terms of confidentiality, although similar considerations apply when considering Security Measures for other purposes.

36. The approach in this document is firstly to group Potential Attackers conceptually according to their most important characteristics, that is, normally Clearance and Technical Factor, ignoring their geographical location and the paths by which they might mount an attack. A group of Potential Attackers consists then of all those Potential Attackers who share the same Clearance and Technical Factor. The possible attack paths for various members of the group may be different, and the Security Measures which block those paths may be different.

37. The analyst may if desired group Potential Attackers according to other characteristics provided this does not significantly increase the number of groups and is not simply a device to reduce the numbers in the groups. If a Potential Attacker has multiple Technical Factors he should be counted in each group.

38. To introduce a further flexibility the analyst may subdivide a small number of the resulting Potential Attacker groups. Not more than 10 such sub-groups should be introduced; they should correspond to real differences in the Potential Attacker characteristics, and sub-groups of a Potential Attacker group should give rise to significantly different Assurance requirements.

39. Although of less significance, grouping is also applied to data. It is appropriate to group data in different ways according to whether the Threat considered is to Confidentiality, Integrity or Availability. In the Confidentiality case, all the data on the system at each protective marking level should be grouped together. It is not generally suitable to group the data according to the particular sub-system on which it is held. Thus, if data of the same sensitivity is distributed across several sub-systems, the

different Security Measures on those sub-systems will all form part of the Security Barrier that protects the data.

40. In the Integrity and Availability cases the data should in general be grouped according to the Impact that compromise would have, that is, the value of the Impact parameter, but data may be grouped on other criteria at the analyst's discretion.

41. Each group of Potential Attackers will then present a Threat to each data group, and each such Threat is addressed by a group of technical measures. This group of measures is, by definition, a Security Barrier. The method works out an Assurance Level for Security Barriers, and the degree of Assurance required in a Security Barrier is determined mainly by the characteristics of the group of Potential Attackers and the characteristics of the data group.

42. As a Security Barrier may consist of several component Security Measures, each part will need to be assured to at least the level for the Security Barrier. It is possible that the same Security Measure may be used by several Security Barriers, in which case it should be assured to the highest calculated level. It is also possible that the Security Measures in a single Security Barrier include all the security functionality of the whole system. In such a case the system is essentially monolithic.

43. To use these grouping options effectively, it is desirable to have an idea of the likely design of the system and the particular Security Measures that will be used. It is envisaged that these Assurance Level calculations will be made iteratively by the system designers as they evolve to a design that can incorporate the required level of security in the most economical way.

44. In the Integrity case, separate Security Barriers define the functionality that prevents the modification of a particular group of data by a particular group of Potential Attackers. It is necessary to stretch the definition of a Potential Attacker group a little to accommodate the possibility that data corruption may sometimes not be attributable to a particular Potential Attacker, that is, data may require protection against unattributable accidents.

45. In the Availability case, a further extension of the Security Barrier concept is necessary. Denial of Service attacks threaten services rather than data. It is therefore necessary for the analyst to define particular groups of services (or sub-services) that require enhanced protection, characterised by the Impact if they are compromised. Then a separate Security Barrier is deemed to protect each service from each group of Potential Attackers. Again such a Barrier may require protection against unattributable accidents.

46. **Networked Systems** It is often hard to define what is meant by ‘a system’. Systems may be definable physically in terms of the hardware and its location, but when two ‘systems' are connected together they may be considered either as ‘two systems connected together’ or ‘one bigger system’. The latter is a more consistent

approach, but runs into problems where part of a system is relatively isolated and it is desired to treat this part in some way differently from the rest of the system. Further guidance on networked systems is given at **Chapter 15**.

47. Focusing on one Security Barrier at a time means that sub-system boundaries need not be rigidly specified: the analysis encompasses the full system, and Assurance can be concentrated in relatively isolated sub-systems. It is however still important to define the total scope of the analysis and what external Security Measures can be assumed to be in place.

48. Accesses involving several interconnected sub-systems are likely to be regulated by separate Security Measures provided by the individual sub-systems. The overall Assurance Level attained by a Security Barrier is determined by the Assurance of its constituent Security Measures and the way they combine into a mutually supportive whole.

49. **Defence in Depth** No Security Measure can be guaranteed to be 100% effective, and at first sight it might appear attractive to present several Security Measures which would have to be breached for an attack to succeed, on the basis that if the first is 99% successful at blocking attacks, and the second 90% effective, then in combination they are 99.9% effective.

50. In practice, achieving this effect in CompuSec is problematic. In many cases the several Security Measures which block an attack path are not truly independent, and breaching one Security Measure leads to ways in which other Security Measures can be circumvented easily. An example is an ID&A followed by Internal Access Controls. If a Potential Attacker can defeat the ID&A, for instance by guessing a user's ID and password, then he has access to all the data to which that user should have access. However it is recognised that in a carefully controlled environment, with well-understood functionality, genuine Defence-In-Depth (DiD) can be achieved.

51. An Accreditor may accept a Defence-in-Depth argument using a series of Security Measures if he is satisfied that the different Security Measures are indeed independent. In such cases the 'effective Assurance Level' of two Security Measures in combination is determined as follows: where each Security Measure is Assured to the same level, the effective Assurance is one higher than that level, otherwise the effective Assurance Level is the higher of the two.

52. It is stressed that the Defence in Depth argument is regarded as providing a functional equivalent of a higher assurance level, and that care must be taken that this should not be misquoted as being "equal to" a higher EAL number.

53. In all cases where a Defence in Depth argument is used within MOD, the exercise of Accreditor discretion must be sanctioned by the Sector Security Authority(s) involved, who will require proof that the mechanisms employed to implement the Barrier Functions (BF) are, indeed, functionally independent in both Implementation and

Operation (e.g. based upon differing paradigms such as stateless and stateful operation). If the calculated assurance requirement being addressed exceeds EAL3.4, or if Compartmented information is involved, the Departmental Security Officer (DSO), as represented by InfoSy(Tech), must also be consulted.

54. **Dilution** Where data at a given level of marking is diluted by a large quantity of data at a lower level of marking there may be a justification for a slight reduction in Assurance Level, but the presence of data at the high level cannot be totally ignored. Dilution can only be allowed when it is substantial, of the order of 0.1%, the difference in marking level is not great and there is no easy way to pick out the more highly marked data.

55. In all cases where a Dilution argument is used within MOD, the exercise of Accreditor discretion must be sanctioned by either the PSyA of the TLB involved, the DSSO, or, if Compartmented information is involved, the Departmental Security Officer (DSO), as represented by InfoSy(Pol), must also be appraised.

56. In all cases the grant of a sanction will require the submission of proof that the dilution is indeed stochastic (random), in both time and space where applicable, and that no additional channels (e.g. descriptive filenames or scan-able labels) exist to subvert the perceived degree of randomness. In this context, Randomness can be considered to be any Pseudo-Random sequence with its auto-correlation function approaching zero (i.e. ≤ 0.025 for $n \leq 1000$ to ≤ 0.005 for $n \geq 1{,}000{,}000$).

Methods Of Analysis

57. The essence of security analysis is to identify all the Risks in terms of the Threats and Vulnerabilities, then to place appropriate Security Barriers to reduce each Risk to an acceptable level. This document does not mandate any particular risk identification method. However, CRAMM is an HMG-preferred analysis tool which aids in detailed analysis and is recommended when advice on specific detailed Security Measures is required. Whatever method of analysis is chosen, it should be methodical and well documented.

58. **Confidentiality** Identification and Authentication, and Access Control Security Measures, together usually form the backbone of protection for the Confidentiality of Data. Generically there are three reasons for preventing access to data. These are related to the Mode of Operation.

59. **Mode of Operation** In a monolithic system, the Mode of Operation reflects the reason for wanting to prevent access to data. The definition of 'Mode of Operation' has been amended in this document to adapt it from a system-wide concept to one that can relate to parts of a system, down to the level of individual Security Barriers. The 'Mode of Operation' of a Security Barrier is then merely a shorthand way of referring to the reason for providing the Security Barrier.

60. The three reasons for preventing access to data are:

a. **Lack of Clearance Level :** The Potential Attacker does not hold the Clearance Level necessary to see protectively marked material. This applies where material is marked using the standard protective markings RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET, and the Potential Attackers lack checks and clearances of: Basic Check, Security Check and Developed Vetting. Systems with internal Access Controls for this reason have a Multilevel Mode of Operation. Security Barriers which are provided for this reason likewise have a Multilevel Mode of Operation.

b. **Lack of Special Access Approval:** The Potential Attacker may lack Special Access Approval which applies to special data (often intelligence material), even though the Potential Attacker is cleared to a sufficient level, under Lack of Clearance Level above, to see the data. This applies where there are formal rules in place for marking such data and formally giving people Special Access Approval to see that data. The system of Special Access Approvals exists locally within Government Departments or occasionally between closely co-operating Government Departments. This includes the use of national caveats, for example, UK/US EYES ONLY, where a Potential Attacker is not one of the appropriate nationalities. Systems which need internal Access Controls solely for this reason have a Compartmented Mode of Operation. Security Barriers which are provided for this reason likewise have a Compartmented Mode of Operation.

c. Need-To-Know: The Potential Attacker may have no Need-To-Know the data. It is likely to be locally determined and is sometimes referred to as a 'Privacy' requirement. It includes the use of the UK EYES DISCRETION marking. Systems with internal Access Controls solely for this reason have a System High Mode of Operation. Security Barriers which are provided for this reason likewise have a System High Mode of Operation.

61. For completeness, systems where all Potential Attackers are excluded by non-technical means, and all users need access to all the data, have a Dedicated Mode of Operation.

62. When assessing the conceptual mode of operation of a Security Barrier which prevents logical access to system by those having physical access, the value used depends on whether the Potential Attacker(s) have an appropriate clearance level, where COMPARTMENTED mode reflects their lack of access approval, or whether the Potential Attacker(s) do not have an appropriate clearance level, in which case the MULTI-LEVEL mode is appropriate.

63. **Integrity** The Integrity of data in a system is always important, but is often taken for granted. The Manual of Protective Security establishes two protection

levels, Baseline for the majority of normal situations, and Enhanced, for special environments or where special risks have been identified.

64. 'Baseline' in this context means those Security Measures which represent industry good practice, which can be regarded for now as being the equivalent of a requirement for those technical measures that would be required under ISO9001 and BS7799.

65. When Enhanced protection is indicated, this document can be used to calculate an Assurance Level. The CRAMM tool can be used for a more detailed analysis of Integrity functionality.

66. The Security Measures supporting Confidentiality may also support Integrity. For instance, access controls may be able to set independent Read, Modify and Write permissions. Important Security Measures include the use of:

a. Anti-virus software, to prevent the import of malicious code ;

b. An inherently non-alterable medium - such as a CD-ROM - to store the data ;

c. A 'master copy' for comparison ;

d. A mathematical checksum to ensure data has not been modified. With many standard data transfer protocols such a checksum is an inherent part of the protocol.

67. Digital signatures may be used where additional Integrity is required. The subject of digital signatures is complex and should their use be contemplated specialist advice from InfoSy(Tech) should be sought.

68. Measures specifically to protect for Integrity are usually determined locally. This document gives guidance later on finding an appropriate Assurance Level should such a Measure be indicated.

69. **Availability** Availability requirements are usually expressed at the system level or at the service level. It is rarely that the concept of Availability is applied to data directly, although Availability of the data may be essential for the Availability of a service or system (Deliberate attacks on Availability are often referred to as Denial of Service attacks).

70. The HMG standards establishes two protection levels, Baseline and Enhanced, and requires system owners to assign their systems to one category or the other. The acceptable level of Availability is an operational matter, and how that Availability is achieved is a design decision. The CRAMM tool can be used for a more detailed analysis of Availability requirements. Although protecting against hardware failure is

outside the formal scope of this document, suitable Security Measures include, in ascending order:

a. Replacement of faulty units from central stores under a 'normal working hours response within n days' support contract ;

b. Replacement of faulty units from locally held supplies by maintenance staff on 24 hour call out ;

c. Cold spare, with manual detection of failure and manual switch-over ;

d. Hot spare with automatic detection of failure and manual switch-over ;

e. Hot spare with automatic detection of failure and automatic switch-over ;

f. Multiply-redundant system with 'majority vote' decision.

71. The Common Criteria provides some functional components:

a. Fault Tolerance - Security Measures that ensure the system will maintain a level of correct operation in the event of failures ;

b. Priority of Service - Security Measures that control the use of resources to ensure that high priority activities will be accomplished without undue interference or delay by low priority activities ;

c. Resource Allocation - Security Measures to prevent the unauthorised monopolising of resources by users.

72. Security Measures specifically to protect Availability are usually determined locally, although in all cases should at least conform to industry good practice, which can be regarded for now as being the equivalent of a requirement for those technical measures that would be required under ISO9001 and BS7799.

73. This document gives guidance later on finding an appropriate Assurance Level should such a Security Measure be indicated.

74. **Security Accounting and Audit** A basic summary of Security Accounting and Audit appears in Guide to the Security of IT Systems. Security Accounting and Audit functions serve four purposes:

a. Detecting unusual activity which may indicate a breach of security - when done in real time this may be equivalent to Intrusion Detection ;

b. Providing 'forensic' evidence ;

c. Deterrence ;

d. Assisting in remedial action when a problem occurs, such as corrupted data.

75. Security Accounting and Audit is a useful Security Measure to counter the threat posed by privileged users, such as system managers, who are able to override normal access controls. On some systems the fact that all such users' actions are accountable may be the only deterrent to such an attack.

76. Experience has shown that in practice Security Accounting and Audit systems are often difficult to operate. Security Accounting logs are difficult to understand and unusual activity which may indicate a breach is usually obscure. Auditing is very time consuming and tedious. Except in a well-disciplined environment Audit is rarely performed effectively.

77. To be of any use, Security Accounting Records need to be audited. The frequency of audit is a matter of judgement for the Accreditor, and will depend on the nature of the business and other local factors. Audits may be manual or tool-based. It is important to determine what constitutes normal behaviour and abnormal behaviour.

78. It is worth noting that there are attack tools for common operating systems which can hide a successful attack by altering the Security Accounting records.

79. This document allows compensation for less than fully effective Security Accounting and Audit by raising slightly the Assurance Level of other Security Barriers. The functionality that can be regarded as fully effective is detailed in the parameters for effective Security Accounting and Audit.

80. **Physical Measures** Physical Security Measures control physical access to hardware such as terminals, servers, cabling, and include building access controls, fences, walls, locks etc. Almost all IT systems will have some physical Security Measures already in place. Interaction between Physical Security Measures and Technical Security Barriers comes about because the Physical Measures both reduce the number of Potential Attackers and limit Potential Attackers to those of known Clearance Status. Some isolated systems may be able to rely almost entirely on physical security.

81. **Personnel Security Measures** The recognised formal checks and clearances for personnel are Basic Check, Security Check, and Developed Vetting. Personnel Security Measures have the effect of restricting normal access to the system to people with known clearances, permitting reasonable assumptions about their reliability.

82. Personnel Security Measures can interact with Technical Security Barriers. There is often an opportunity to reduce the required Assurance Level of the Technical Security Barriers significantly, or even remove them, by increasing the clearance of Potential Attackers. This reduces required Assurance Levels in its own right and may well change the Mode of Operation, resulting in a further reduction in required Assurance Levels.

83. A reduction in Assurance Level is allowed if personnel are cleared to a higher level than they strictly need to see the data, which is incorporated in the Worksheets.

84. **Procedural Security Measures** Procedural Security Measures aim to reduce risks by applying 'rules', and are usually locally devised and approved. There are occasions when a procedural rule may be invoked which reduces or removes the need for some particular Technical Security Measure, for instance a 2-man rule may be considered adequate to prevent an attacker mounting any attack on an Access Control Security Measure.

85. Accreditors will need to use their discretion when considering the effectiveness of Procedural Security Measures and any consequential reduction in other Security Measures, and may need to seek advice from InfoSy(Tech).

86. **Encryption** An important Security Measure to reduce the risk of interception is the use of encrypted lines using HMG-approved cryptographic equipments ("cryptos"). An approved crypto used in accordance with CESG Infosec Memorandum No 3 (British Cryptographic Instructions) can be assumed to be totally effective in maintaining the Confidentiality of the data from an interception attack.

87. If communications paths are accessible to the public, as is often the case, using an appropriate grade of crypto immediately reduces (effectively to zero) both the Threat to the data in transit and the Threat to Confidentiality of the end systems via the communications path. More information on the use of cryptos is available in Infosec Memorandum 3.

88. Encryption of data stored in a system is an appropriate Security Measure to counter the Threat that a whole system will be lost or captured intact and hence applies particularly to portable computers. In other cases, experience has shown that wholesale encryption is difficult to implement and manage, and the gains are less than might be expected. Further advice on the use of encryption for internal access control may be obtained from InfoSy(Tech).

Baseline Compusec Functionality Requirements

89. In the majority of cases there should be:

a. An Identification and Authentication Measure

b. Internal Access Control Measures - these may be Mandatory Access Control and/or Discretionary Access Control, depending on the reason for the Security Measure

c. Where feasible, a Security Accounting and Audit Measure - where none is present, there may be a consequential increase in the Assurance Level of related Security Barriers and in some cases, additional Security Measures specifically to ensure the:

i. Integrity of data over and above commercial standards ;

ii. Availability of data or a service over and above commercial standards.

90. The following paragraphs elaborate on this point.

91. **Identification and Authentication (ID&A)** All systems should have the following functionality:

a. Up-to-date lists of authorised users ;

b. Positive identification of all users at the start of each processing session;

c. Authentication of computer connections via communications circuits before transmission. This may be provided by cryptographic protection of the circuit.

92. Passwords are part of most ID&A Security Measures. Specific requirements relating to passwords and their generation and management are given Chapter 6, supplemented by CESG CompuSec Memorandum No 8 (Password Guidelines) if required.

93. **Internal Access Control - DAC and MAC** All systems, except the few working in Dedicated Mode, need internal Access Controls to prevent Potential Attackers from reading, modifying, or otherwise interacting with the data.

94. This document cannot describe the detailed functions that must be provided for this purpose. As a general rule, any communication path between a Potential Attacker and the data can be used to carry an attack or leak data. It is for the system designers and implementers to identify all possible means of attack and ensure that they are blocked. It is precisely because this is a difficult and error prone task that Evaluation and Certification can add value to the procurement process.

95. In a Discretionary Access Control (DAC) system, a user can be given the right to access data by any other user who already has access. In a Mandatory Access

Control (MAC) system, an ordinary user cannot give another user access rights; this provides protection against careless or malicious users and also against malicious code that attempts to mimic the actions of users.

96. Traditionally MAC has been implemented by operating systems that assign protective marking labels to data and permit access only when user clearances are consistent with protective marking. There is no requirement for this specific implementation if the required protection can be provided in other ways. The most common alternative is trusted downgrade or trusted release, whereby DAC is provided within security domains, and data is transferred between domains or released only by the actions of specifically authorised staff.

97. Technical Security Measures (trusted paths) ensure that the actions are performed by people rather than by malicious code, and carelessness and malice are deterred by a higher level of Accounting and Audit.

98. Where the Potential Attacker has the required Clearance Level or Special Access Approval for the data but may lack a Need-to-Know, the use of DAC is permissible. Where the Potential Attacker does not have the required Clearance Level or Special Access Approval for the data (Multilevel or Compartmented Mode of Operation), MAC is required. This is summarised in the following table :

Associated Mode of Operation	Type of Internal Access Control Measure
Multi-level	MAC
Compartmented	MAC
System High	DAC
Dedicated	None

99. Where the presence of nationally caveated material, for example, UK/US EYES ONLY, calls for a Compartmented Mode of Operation, and hence calls for MAC, there are subtle points of interpretation. The definition of UK EYES ONLY permits the originator, and only the originator, to extend access to the material. It is difficult to design systems which provide originators with this freedom. This conflict may be resolved by Procedural Security Measures.

100. **Integrity** No special Technical Integrity Measures are usually needed because the Access controls described above can be configured to control 'write' and 'modify' permissions as well as the 'read' permissions needed for Confidentiality. If this does not apply, then specific Integrity Protection Measures may be needed.

101. Should a Technical Security Measure (such as a checksum algorithm or an Access Control Measure) be indicated to protect data Integrity, then the appropriate Assurance Level for that Security Measure can be calculated by using the method in the Worksheets.

102. **Availability** No special Technical Availability Measures are usually needed as this is a local operational matter. Should a Technical Security Measure (such as an automatic backup, or automatic switch-over to a 'hot spare') be indicated to protect Availability then the appropriate Assurance Level of that Security Measure can be calculated by using the method in the Worksheets.

103. **Integrity & Availability** In addition to any Technical Security Measures for Integrity and Availability, the following supporting measures should be considered, based upon the Criticality Level of the system :

Criticality Level	Objective	Countermeasures
CL1	Provide sufficient countermeasures for additional protection against special risks or special threats (accidental or malicious), where consequences of failure would be as given by Impact	• As CL2, plus : • Protection against radiated energy attack • Fully meshed communications links with at least 50% utiising dedicated bearers • Diverse processing capacity
CL2		• As CL3, plus : • Flexible Power backup • Multiple, diverse routed communications links • Redundant processing capacity
CL3		• As CL4, plus : • Specific checking for malicious code • GFE Authentication • Short term backup power • Data backup with remote storage • Fallback communications links • Standby processing capacity
CL4	Provide general protection against normally forseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations)	• Defined Contingency Plan • Data backup with local storage • COTS Anti Virus Software • COTS Authentication

104. **Security Accounting and Audit** The term 'Accounting and Audit' in this document refers only to general purpose Security Accounting and Audit, that is, the

recording of actions and events that may indicate attempts to circumvent ID&A or Access Controls. There may well be requirements for other types of accounting and audit - such as financial audit, or audit needed for local business management reasons - which exceed those stated below but are outside the scope of this document.

105. Normally an Security Accounting and Audit system will be required. Where a Security Accounting and Audit system is lacking, and this increases the reliance placed on associated Security Barriers, then the calculated Assurance Level of those Security Barriers is increased. (Depending on rounding, this may or may not increase the required Assurance Level.)

106. In this document the treatment of Security Accounting and Audit is separated into two aspects: firstly the minimum recommended Security Accounting and Audit functionality, and secondly the effect the presence (or absence) of Accounting and Audit functionality may have on the required Assurance Level of other Security Measures. The first of these uses the term 'Security Accounting and Audit Rating', the second uses the term 'Accountability'.

107. The specific events to be included in the Security Accounting depend on the 'Security Accounting and Audit Rating' as derived from the table below.

Clearance Status of Potential Attackers	**DV**	**SC**	**BC**	**Uncleared**
TOP SECRET	Comprehensive	Comprehensive	Comprehensive	Comprehensive
SECRET	Comprehensive	Comprehensive	Comprehensive	Comprehensive
CONFIDENTIAL	None	None	Partial	Comprehensive
RESTRICTED	None	None	None	Partial

108. The Security Accounting and Auditing system itself may need Certification, and the Assurance Level can be calculated by using the method in the worksheets.

109. When an event is to be recorded at least the following elements should be logged:

- Type of event
- User ID
- Date and time
- Device ID, if relevant

110. The Security Officers(s) should be able to print an easily readable report of all or selected events.

111. Events To Be included in the Security Accounting Record

None	There is no mandated requirement but, as mentioned above, there may be a local or departmental requirement for audit.
Partial	The following should be recorded, if applicable to the system under consideration: • all logon attempts whether successful or not • log off • creation, deletion or alteration of access rights and privileges • creation, deletion or alteration of passwords • creation, deletion or alteration of the Security Accounting log.
Comprehensive	The following should be recorded, if applicable to the system under consideration, in addition to the partial requirements: • production of protectively marked hard or soft copy output • creation or deletion of files and the assigning of their level of protective marking • any re-grading of the level of protective marking either of data objects or logon privileges • introduction or removal of storage media • backup operations • attempts to access data/files and whether or not successful • attempts to disseminate data/files whether or not successful.

112. The frequency and type of audit is a matter of judgement for the Accreditor or DSO, and will depend on the nature of the business and other local factors. The basic recommendation is that effective Audit should take place at adequate intervals.

113. **Data Exchange** In most systems data will be moved around and may be exchanged with other systems. Maintaining the Confidentiality, Integrity and Availability of transferred data may need special Security Measures. Many protocols exist which ensure data Integrity during transfer. HMG-approved cryptos can be used to ensure Confidentiality during transfer. Various forms of redundancy can be used to ensure system or data

114. Should a (non-cryptographic) Technical Security Measure be considered necessary to protect either the data being exchanged or the whole system, then it will protect either the Confidentiality, Integrity or Availability (or combinations of these) and the appropriate Assurance Level for that Security Barrier can be calculated by using the methods in the worksheets.

115. Additionally, to facilitate interconnection between systems, some common assumptions as to available security functionality is required, as detailed at **Chapter 13**.

Parameters And Their Values

116. The level of risk presented to system data by a group of Potential Attackers depends upon various characteristics of the system, its data, and the attackers themselves. There are many possible ways of describing these characteristics. In this Section a standardised set of parameters is defined and discussed in some detail.

117. There are two special cases where it may not be obvious what the parameter values should be where there is:

a. Public physical or logical access to a system ;

b. A danger of a breach of security from the accidental failure of the Security Measure, that is, a failure not caused by a Potential Attacker.

118. The parameter values for these two special cases are stated explicitly where appropriate. The term ‘public physical access’ applies where a terminal or part of the system is placed in a public space where there is uncontrolled access, such as a public library. ‘Public logical access’ is where there is the possibility of accessing the system via another system, such as the Public Switched Telephone Network (PSTN), to which the public has access.

119. Although Potential Attackers will have been grouped on the basis of their most important common characteristics, they can be expected to differ in minor parameters. This raises the question of what values of these parameters to assign to the group as a whole. The general guidance is to assign the typical, or average, value, rather than the worst case. If it is particularly difficult to decide on a typical value, then the limited dispensation to subdivide the group should be. In a ‘monolithic’ calculation, use worst-case values for Protective Marking and Clearance.

120. The parameters are:

- Environmental Factor
- number of Potential Attackers
- Check and Clearance Status of the Potential Attackers
- protective marking level of the Data (for Confidentiality)
- impact (for Integrity or Availability)
- Mode of Operation
- Technical Factor, which consists of :

- Facilities Available

- Cumulative Opportunity

• Level of Publicity of the existence of the data

• Accountability

• Quantity of Data

121. **Environmental Factor** This parameter is needed for all Groups of Potential Attackers. It is an empirical reflection of certain factors known to have a bearing on the likely Threat to be associated with that Group. Such factors will typically have been identified in national threat assessments, and may be complemented by local evidence of particular problems known to departments. Possible values are:

Normal	Default value
Increased	Appropriate if any of the following is true: • a department has evidence of a persistent problem relevant to the Group, for instance recurrent fraud, internal hacking, infringements of departmental rules, or some other form of 'bad track record' • the Group is outside the UK • there is some reason to believe the Group may be a target of foreign intelligence
High	Appropriate if any of the following is true: • the Group has a connection to a public network, the major instance being the Internet • the Group is outside the UK in a place where it is a target of an aggressive intelligence service

122. It is important that where any direct or indirect connection to public networks is identified as a result of this analysis, an explicit statement as to its presence must be made in association in presentation of the results of the Risk Analysis to Accreditors. If Virtual Private Networking (VPN) technology is used, it may not be apparent whether or not such direct or indirect connection to public networks exists.

123. Client-Server VPN (CSVPN), which use encrypted tunnelling either between hosts or between clients and hosts, with encryption under the control of the System Management Authority, are analogous to Link Encryption and can be considered to be provided link level protection commensurate with the Grade of cryptography available, and thus provides separation from public networks.

124. On the other hand, Service Provider Furnished VPN (SPFVPN) can be implemented by either Cryptographic or Closed User Group (CUG) mechanisms,

outside the control of the System Management Authority, and as such can only be considered to provide isolation from public networks if both the specific architecture can support this concept, and an appropriate level of trust can be demonstrated in the Service Provider.

125. In addition to the generic Environmental Factors laid down, certain classes of MOD systems have specific Environmental Factors, based upon their Criticality Level (CL):

Criticality Level (CL)	Environmental Factor
1	High
2	Increased

126. Advice can be obtained from the JSyCC office within DDefSy as to threats to specific MOD locations or formations.

127. For cases where the Security Barrier protects against an accidental breach of security the value is Normal.

128. The numerical value to be used in calculations derived from this parameter is found on the working chart.

129. This parameter can alter the Assurance Level by up to 1.0.

130. **Number of Potential Attackers** This parameter is needed for all cases.

131. Values are 1-10, 11-50, 51-200, 201-1000, 1001-5000, greater than 5000

132. Where there is public physical or electronic access, the value is greater than 5000.

133. Where precise connections of Potential Attackers are not known, for example when the system is frequently reconfigured, or connected to other systems that are imperfectly understood, a conservative (high) value should be used. If the value of >5,000 is selected, this will have the effect to Saturating the factor in the analysis, and will thus provide "future-proofing" against any subsequent use of cascade connections either within or without the system management(s)' control.

134. For cases where the Security Barrier protects against an accidental breach of security, in the confidentiality case the value is that appropriate to the number of people who would be in a position to exploit the breach. For example, if the accident were to release the information to the public, the value would be >5000, but if only to one individual, then the value would be 1-10. In the Integrity, Availability and Accounting and Audit cases, where there is no obvious group of people who might exploit a failure, the value >5000 should be used.

135. As explained above, Potential Attackers are grouped, and the number in each group is input to the calculation.

136. The numerical value to be used in calculations derived from this parameter is found on the appropriate working chart - refer to Appendices 1-4.

137. This parameter can alter the Assurance Level by 2.

138. **Check and Clearance Status of Potential Attackers** This parameter is needed in all cases.

139. This is the normal Clearance Level of the Potential Attackers and can have the values Uncleared, Basic Check (BC), Security Check (SC), Developed Vetting (DV). In this document the term Basic Check includes complying with any checks made which are locally approved and are broadly comparable to a formal Basic Check.

140. Where the public have physical or electronic access to the system but are to be excluded by the Security Barrier under consideration from access to some parts of the system, the value is Uncleared.

141. Where the Security Barrier is protecting against an accidental breach of security, for the confidentiality case the value is that appropriate to the people who would gain by the occurrence of the breach, for example, if some users are DV and some BC, and a failure of the Security Barrier would allow TOP SECRET material to fall into the hands of the BC users, then the value is BC. For the Integrity, Availability and Accounting and Audit cases there is no obvious group of people who would gain by the occurrence of a breach, the appropriate value is Uncleared.

142. This parameter can alter the Assurance Level by 6.

143. **Protective Marking of Data** This parameter is needed only for the Confidentiality and Security Accounting & Audit cases.

144. This is the normal protective marking and can have values:

- RESTRICTED
- CONFIDENTIAL
- SECRET
- TOP SECRET

145. This parameter can alter the Assurance Level by 7.

146. **Impact** This parameter is needed only for Integrity or Availability cases, and possible values are Minor, Significant, Major, Extreme. The various values relate to the impact resulting from a loss of Integrity or loss of Availability. This parameter is similar to the Protective Marking Level for the Confidentiality case.

147. MOD systems should be assessed for a Criticality Level (CL), the details of which are included in Chapter 1 :

Criticality Level	Protection Category	Impact Parameter
CL1	Enhanced	Extreme
CL2	Enhanced	Major
CL3	Enhanced	Significant
CL4	Enhanced	Minor

148. Note that this parameter reflects only the effect of loss of Integrity or Availability, not the protective marking of the data which normally reflects the effect of loss of Confidentiality. Thus it would be possible to have data marked TOP SECRET but with an Impact of Minor should its Integrity be lost, and vice-versa.

149. Only the more immediate effects should be considered; remote consequences which would require a long chain of unlikely events should be ignored.

150. **Mode of Operation** The Mode of Operation of the Security Barrier under consideration applies in the Confidentiality case only and is determined from the reason for providing the Security Barrier - refer to paragraph 64 - and summarised in table below.

Reason for Security Barrier	Associated Mode of Operation
Lack of Clearance Level	Multi-level
Lack of Special Access Approval	Compartmented
Protecting nationally caveated material (e.g.UK EYES ONLY, UK/US EYES ONLY) from nationals of other countries	
Lack of Need-To-Know	System High
Protecting UK EYES DISCRETION from non UK nationals	

151. **Technical Factor** This parameter is needed for all cases.

152. The Technical Factor is an important parameter that reflects the constraints, imposed by the system or its environment, on the ability of a Potential Attacker to mount an attack. If a Potential Attacker has limited facilities available to mount, and little opportunity for, an attack, then the Technical Factor is low. If a Potential

Attacker has many facilities available and unlimited opportunity for attack, then the Technical Factor is high.

153. The Technical Factor is determined by a combination of the partial parameters Facilities Available and Opportunity for Attack.

154. It may be that a Potential Attacker has several interfaces directly available, providing him with widely differing facilities and opportunities. These interfaces should in principle be regarded as relating to differing Security Barriers, and the Potential Attacker should be counted as attacking each Security Barrier (that is, he should be counted many times). However, it is quite likely that the same Security Measures will be present in each Security Barrier; the highest assurance requirement then applies.

155. More complicated scenarios are also quite common: one interface may give a Potential Attacker access to a more restricted interface. If there is no potential for subverting the more restricted interface then its Technical Factor should be used. For example, a Potential Attacker may have unrestricted access (high Technical Factor) to a PC, but only receive broadcast teletext messages on it. Clearly he can do nothing to influence the second computer that generates the messages. However, if his PC has a trusted connection to the second computer, but the software provided on the PC is only able to request the teletext message the situation is very different. He can very easily introduce new software and increase the technical factor at the interface. Therefore, if one interface gives access to functionality that protects the second more restricted interface, then that functionality must be assured to the level determined by the Technical Factor at the first interface. Only then can the Technical Factor at the second interface be used to determine the assurance required of any further functionality.

156. **Facilities Available** The value for the Facilities Available represents the Potential Attacker's capability at the target of attack. Determining the value for this parameter requires considerable judgement. Guidance on the appropriate value is given in the lists below, but if the actual facilities available to a Potential Attacker are not listed then either an informed estimate of the nearest equivalent should be made, or the Security Authorities consulted.

157. Not all the facilities on the system need to be taken into account, but only those facilities which the Potential Attacker can bring to bear on the Security Barrier under attack.

Very Limited	Situations in which Potential Attackers have very limited capability at the target of attack, typically where no more than the following facilities are available: • communications only • E-mail without the possibility of any attachments or macros • receive-only terminals • Potential Attackers presented with a Logon Screen protected by a User identification and Password Measure conforming to **Chapter 6 Annex A**
Limited	Situations in which Potential Attackers have limited capability at the target of attack, typically: • simple office automation facilities, for example, word-processing, E-mail with non-executable attachments and no facility to run macros, diary facilities, appointment scheduling • menu-driven captive applications.
Normal	Situations in which Potential Attackers have significant capability at the target of attack, typically: • operating system accessible to Potential Attackers • E-mail with executable attachments • Potential Attackers presented with a Logon Screen protected by a User Identification and Password Measure not conforming to **Chapter 6 Annex A** • macro, database or Fourth Generation Languages (4GL) available • floppy disk drive where there are other Security Measures in place (such as a 2-man rule) to prevent software being introduced via, or the computer being booted from, the floppy disk drive.
Extensive	Situations in which Potential Attackers have extensive capability at the target of attack, typically: • full compilers and program development facilities which potentially support attacks on Security Barriers • automated penetration tools • network analysis tools • packet sniffing software • floppy disk drive where there is no Security Measure in place to prevent software being introduced via the floppy disk drive.

158. For cases where the Security Barrier protects against an accidental breach of security the value is Very Limited.

159. For most modern standard office automation facilities the value Normal is appropriate. This includes cases where there are limited compilers associated with the office automation system.

160. Where an assertion is made that User identification and Password Measure conforming to **Chapter 6 Annex A** are used, separate calculations must thereafter be

performed for each instance of the Password Measure in addition to that for the barrier under consideration. This calculation is to be performed with the value of the Facilities Available parameter set at a level appropriate to the system architecture if the password mechanism were not in place, and the resultant calculated assurance level for each such calculation be used in determining the Password Measure from **Chapter 6 Annex A**.

161. It is stressed that in addition to any ITSEC evaluation requirement the subject Barrier may attract, the use of this CESG password measures will also require that CESG Review and Approve the use implementation of the Password. It should also be remembered that supporting ESE measures for the Protection of Software Cryptographic Modules as laid down at **Chapter 6** will be required.

162. Where an assertion of "communications only" is proffered, further consideration of the nature of the interaction predicated by the system's Information Exchange Requirements (IER), characterised in terms of NATO Interoperability Planning Document (NIPD) Levels, is required to described the nature of the communications channel presented to the Barrier and thus the "facilities available" :

NIPD Level	Channel Type	Facilities Available
5B	Internet Protocol suite	Extensive
	Other Channels	Normal
	Encrypted or "tunnelled"	Very Limited
5A	Internet Protocol suite	Extensive
	Other Channels	Limited
	Encrypted or "tunnelled"	Very Limited
4	Internet Protocol suite	Extensive
	Other Channels	Very Limited
≤3	Manual interfaces and "air gaps"	Very Limited

163. **Cumulative Opportunity** The Cumulative Opportunity parameter reflects the cumulative amount of time available to a Potential Attacker to mount an attack. If the level of supervision, such as a two-man rule, is such that an attack could not be mounted unobserved then this should be taken into account and the parameter value reduced accordingly.

164. When applied to a group of Potential Attackers the Cumulative Opportunity value is determined by the worst case individual of the group, with no "collusion" assumed. A rough estimate erring on the cautious (high) side is acceptable.

165. The period over which the opportunity should be calculated is the estimated lifetime during which the protectively marked information will need to be protected (the perishability). If there is regular audit of the system's activity, such that any attempts to breach security are likely to be detected, then the value may be set to reflect the interval between audits.

166. Possible values are:

- <1 hour
- 1-5 hours
- 5-20 hours
- 20-80 hours
- >80 hours

167. For cases where the Security Barrier protects against an accidental breach of security the value is >80 hours. The Default value is >80 hours.

168. **Technical Factor Value** The Technical Factor parameter is calculated in the worksheet from the Facilities Available and Opportunity for Attack. It can alter the Assurance Level by 4.

169. **Level of Publicity** This parameter is needed for all cases. It is an estimate of how well-known the existence of the data is, or may reasonably become, to the Potential Attackers. The possible values are:

Concealed	Where it is unlikely that Potential Attackers of the Data via the Security Barrier under consideration will be aware of the existence of the Data.
Known	Where the Potential Attackers are likely to be generally aware of the presence of the data but would not know its network address.
Publicised	Where the Potential Attackers will be aware of the exact nature and approximate network address of the data.
Advertised	Where the Potential Attackers will be aware of the exact nature and network address of the data.

170. For cases where the Security Barrier protects against an accidental breach of security the value is Concealed.

171. The numerical value to be used in calculations derived from this parameter is found on the working chart.

172. The default value is Known.

173. If invoking the Dilution principle then the Sector Security Authorities will advise a suitable value for this parameter .

174. This parameter can change the Assurance Level by 0.9.

175. **Accountability** This parameter is needed for all cases. It takes account of the presence, or absence, of a Security Accounting and Audit Measure.

176. For normal situations, possible values are:

None	Where there is no effective Security Accounting and Audit
Partial	Security Accounting and Audit believed to be effective is present but does not supply all the functionality - refer to paragraph 101
Comprehensive	A Security Accounting and Audit system supplying all the functionality - refer to paragraph 101

177. Note that the value of the Security Accounting and Audit Rating is irrelevant in determining this parameter. To qualify for a value of Comprehensive all the functionality must be provided, irrespective of the fact that the Security Accounting and Audit Rating may have a value of 'partial' or 'none'.

178. It is noted that in some case the accountability may not be technically achievable. In particular, the widely used Windows NT™ operating system, even with Security Extensions, does not completely meet the specification for Comprehensive. For "vanilla" NT based systems, the Partial Accountability parameter of –0.3 should be used within the worksheets, and if NT(SE) has been implemented, a specific Accountability parameter of –0.5 should be used within the worksheets.

179. In all other cases, the exercise of Accreditor discretion must be sanctioned by the Sector Security Authority(s) involved, who will require proof that the requirement is technically either unachievable or inappropriate, and that appropriate Procedural Measures are in place to compensate. If Compartmented information is involved, the Departmental Security Officer (DSO), as represented by InfoSy(Pol), must also be appraised.

180. There will be abnormal situations where the functionality is not applicable. In these cases a value of Comprehensive may still be appropriate if all the security relevant actions are recorded and will routinely be audited.

181. Any Security Accounting and Auditing facility may itself need Certification, and the Level of Assurance is determined later in the worksheets.

182. The numerical value to be used in calculations derived from this parameter is found on the working chart. The default value is None. This parameter can alter the Assurance Level by 0.6.

183. **Quantity of data** This parameter is needed for the Confidentiality case only. For other cases it should be set to the >1G value.

184. This parameter reflects only the quantity of data being protected by the Security Barrier under consideration. The basis is that a large amount of data is more attractive than a small amount. The Assurance Level calculation is not very sensitive to this parameter.

185. The parameter has possible values <30K Bytes, 30K-1G Bytes, >1G Bytes.

186. For most systems the value will be the maximum of >1G, but the parameter allows a small reduction in Assurance Level where only very small quantities of data are present.

187. If it is felt that the reduction in Assurance Level for a small Quantity of Data is not justified, then the default value of >1G may be used.

188. The numerical value to be used in calculations derived from this parameter is found on the working chart.

189. This parameter can reduce the Assurance Level by 0.6.

Calculating Assurance Levels

190. **Initial analysis** First of all, analyse the system to ascertain whether all assets needing protection are indeed protected by a Security Barrier. A network diagram may help in this process. An alternative approach using the DERA Domain Notation is given at Appendix 5.

191. Identify which assets are to be protected by the Security Barrier under consideration. For the Confidentiality case the assets will be protectively marked data.

192. **Grouping of Potential Attackers and Data** Potential Attackers are to be grouped according to their most important characteristics.

193. A similar grouping process is applied to data, normally on the basis of protective mark-ing (in the Confidentiality case) or on other criteria according to the assessor's discretion in other cases.

194. **Worksheets** Filling in the worksheets is generally quite straightforward. Analysts are encouraged not to agonise unduly if the appropriate value is not obvious, but initially to make a judgement, erring on the cautious side, then reconsidering values if justified and desired. When recording calculations the reason for choosing particular values should be stated, and ‘worst case assumed’ is an acceptable reason.

195. In principle, a separate calculation is required for each Security Measure or Security Barrier.

196. The procedure in every case is to work down the list of parameters in the left-hand column of the worksheets, circling or highlighting appropriate values in the next column.

197. Column 3 translates this into a numerical value, which is then entered in the final column for calculation. For some parameters, column 3 involves a sub-calculation using 2 self-explanatory inputs to provide a single number for column 4.

198. Add up the numbers in column 4. This produces a calculated EAL, which is then rounded to the nearest whole number to give the required EAL.

199. The table below shows the correspondence with ITSEC E-levels.

Common Criteria EA Level	ITSEC E-Level
EAL1	No direct equivalent
EAL2	E1
EAL3	E2
EAL4	E3
EAL5	E4
EAL6	E5
EAL7	E6

200. **CompuSec Target of Accreditation** Having derived the calculated assurance level, this needs to be translated into a practical Target of Accreditation (TOA). For MOD CIS, a number of predefined TOA groupings are defined to scope the assurance activities that will be required:

a. **Best Current Practice (BCP) TOA** (EAL ≤0.0) Even when there is no need for any Government level of assurance, due diligence should be exercised in the implementation of CompuSec functionality, in line with Best Current Practice (BCP). This will include consideration of all relevant public standards, such as Internet Engineering Task Force (IETF) Requests For Comments (RFC) and vendor furnished security guidance ;

b. **MOD Baseline Protection (BP) TOA** (EAL 0.0 – 1.4)

- Either:

  - Use Approved or Certified Products, as included in the Assured Products List (UKSP 06) into the system in the appropriate place to provide all the security functionality required - care is needed to ensure that the product is configured correctly and used within the scope of its Certification Report;

- Or:

  - Have an "IT Security Health Check", consisting of an ESE Verification (EV) and Vulnerability Analysis (VA) by Competent Bodies recognised by the Security Authorities, as laid down at **Chapter 12**, performed ;

c. **MOD Enhanced Protection (EP) TOA** (EAL 1.5 – 3.4)

- Either:

  - Use Approved or Certified Products, as included in the Assured Products List (UKSP 06) into the system in the appropriate place to provide all the security functionality required - care is needed to ensure that the product is configured correctly and used within the scope of its Certification Report; and

  - Have an "IT Security Health Check", consisting of an ESE Verification (EV) and Vulnerability Analysis (VA) by Competent Bodies recognised by the Security Authorities, as laid down at **Chapter 12**, performed ;

- Or:

  - Arrange for the system to be evaluated and certified under the ITSEC, Common Criteria, or other CESG recognised schemes with each component evaluated to at least the level indicated ;

d. **MOD High Protection (HP) TOA** (EAL 3.5 – 5.4)

- Either:

  - Incorporate Approved or Certified Products, as included in the Assured Products List (UKSP 06), certified to the level indicated by the calculation, into the system in appropriate places, where available; and

  - Have a System Evaluation performed under the ITSEC, Common Criteria, or other CESG recognised schemes to confirm the soundness of the configuration ;

- Or:

- Arrange for the system to be evaluated and certified under the ITSEC, Common Criteria, or other CESG recognised schemes with each component evaluated to at least the level indicated;

e. **MOD Special Protection (SP) TOA** (EAL 5.5 or more)

- Consult InfoSy(Tech) before proceeding any further

APPENDIX 1 TO ANNEX B TO CHAPTER 6

Worksheet for calculating required confidentiality assurance level						
		Clearance Status				
Parameters	**Values**	**UC**	**BC**	**SC**	**DV**	**Values**
Protective Marking	RESTRICTED	1.2	-1.6	-3.0	-4.4	
	CONFIDENTIAL	2.9	0.4	-0.8	-2.1	
	SECRET	4.5	2.3	1.2	0.1	
refer to paragraph 143	TOP SECRET	6.2	4.3	3.3	2.4	
Mode of Operation	Multi-Level	0.0				
	Compartmented	0.0				
refer to paragraph 150	System High	-1.0				
Environmental Factors	High	1.0				
	Increased	0.5				
refer to paragraph 121	Normal	0.0				
Number of Potential Attackers	>5,000	2.0				
	1,001-5,000	1.6				
	201-1,000	1.1				
	51-200	0.8				
	11.50	0.4				
refer to paragraph 130	1-10	0.0				
Facilities Available - *refer to paragraph 156*		**VL**	**L**	**N**	**E**	
Cumulative Opportunity	<1 hour	-2.0	-1.0	0.0	1.0	
	1.5 hours	-1.7	-0.7	0.2	1.2	
	5-20 hours	-1.5	-0.5	0.5	1.5	
	20-80 hours	-1.2	-0.2	0.7	1.7	
refer to paragraph 163	>80 hours	-1.0	0.0	1.0	2.0	
Level of Publicity	Concealed	-0.3				
	Known	0.0				
refer to paragraph 169	Publicised	0.3				
Accountability	None	0.0				
	Partial	-0.3				
refer to paragraph 175	Comprehensive	-0.6				
Quantity	>1 GByte	0.0				
	1GByte - 30 KBytes	-0.3				
refer to paragraph 183	<30 KBytes	-0.6				
					Calculated EAL	

System:
Confidentiality Barrier:
Calculated by:
Date:

This page is intentionally left blank

APPENDIX 2 TO ANNEX B TO CHAPTER 6

Worksheet for calculating required integrity assurance level

Parameters	Values	Clearance Status UC	BC	SC	DV	Values
Impact	Minor	1.2	-1.6	-3.0	-4.4	
	Significant	2.9	0.4	-0.8	-2.1	
	Major	4.5	2.3	1.2	0.1	
refer to paragraph 146	Extreme	6.2	4.3	3.3	2.4	
Environmental Factors	High	1.0				
	Increased	0.5				
refer to paragraph 121	Normal	0.0				
Number of Potential Attackers	>5,000	2.0				
	1,001-5,000	1.6				
	201-1,000	1.1				
	51-200	0.8				
	11.50	0.4				
refer to paragraph 130	1-10	0.0				
Facilities Available - *refer to paragraph 156*		**VL**	**L**	**N**	**E**	
Cumulative Opportunity	<1 hour	-2.0	-1.0	0.0	1.0	
	1.5 hours	-1.7	-0.7	0.2	1.2	
	5-20 hours	-1.5	-0.5	0.5	1.5	
	20-80 hours	-1.2	-0.2	0.7	1.7	
refer to paragraph 163	>80 hours	-1.0	0.0	1.0	2.0	
Level of Publicity	Concealed	-0.3				
	Known	0.0				
refer to paragraph 169	Publicised	0.3				
Accountability	None	0.0				
	Partial	-0.3				
refer to paragraph 175	Comprehensive	-0.6				
				Calculated EAL		

System:
Confidentiality Barrier:
Calculated by:
Date:

This page is intentionally left blank

APPENDIX 3 TO ANNEX B TO CHAPTER 6

Worksheet for calculating required availability assurance level						
		Clearance Status				
Parameters	**Values**	**UC**	**BC**	**SC**	**DV**	**Values**
Impact	Minor	1.2	-1.6	-3.0	-4.4	
	Significant	2.9	0.4	-0.8	-2.1	
	Major	4.5	2.3	1.2	0.1	
refer to paragraph 146	Extreme	6.2	4.3	3.3	2.4	
Environmental Factors	High	1.0				
	Increased	0.5				
refer to paragraph 121	Normal	0.0				
Number of Potential Attackers	>5,000	2.0				
	1,001-5,000	1.6				
	201-1,000	1.1				
	51-200	0.8				
	11.50	0.4				
refer to paragraph 130	1-10	0.0				
Facilities Available - ***refer to paragraph 156***		**VL**	**L**	**N**	**E**	
Cumulative Opportunity	<1 hour	-2.0	-1.0	0.0	1.0	
	1.5 hours	-1.7	-0.7	0.2	1.2	
	5-20 hours	-1.5	-0.5	0.5	1.5	
	20-80 hours	-1.2	-0.2	0.7	1.7	
refer to paragraph 163	>80 hours	-1.0	0.0	1.0	2.0	
Level of Publicity	Concealed	-0.3				
	Known	0.0				
refer to paragraph 169	Publicised	0.3				
Accountability	None	0.0				
	Partial	-0.3				
refer to paragraph 175	Comprehensive	-0.6				
					Calculated EAL	

System:
Confidentiality Barrier:
Calculated by:
Date:

This page is intentionally left blank

APPENDIX 4 TO ANNEX B TO CHAPTER 6

Worksheet for calculating required accounting and audit assurance level

Parameters	Values	Clearance Status UC	BC	SC	DV	Values
Protective Marking	RESTRICTED	1.2	-1.6	-3.0	-4.4	
	CONFIDENTIAL	2.9	0.4	-0.8	-2.1	
	SECRET	4.5	2.3	1.2	0.1	
refer to paragraph 143	TOP SECRET	6.2	4.3	3.3	2.4	
Environmental Factors	High	1.0				
	Increased	0.5				
refer to paragraph 121	Normal	0.0				
Number of Potential Attackers	>5,000	2.0				
	1,001-5,000	1.6				
	201-1,000	1.1				
	51-200	0.8				
	11.50	0.4				
refer to paragraph 130	1-10	0.0				
Facilities Available - ***refer to paragraph 156***		**VL**	**L**	**N**	**E**	
Cumulative Opportunity	<1 hour	-2.0	-1.0	0.0	1.0	
	1.5 hours	-1.7	-0.7	0.2	1.2	
	5-20 hours	-1.5	-0.5	0.5	1.5	
	20-80 hours	-1.2	-0.2	0.7	1.7	
refer to paragraph 163	>80 hours	-1.0	0.0	1.0	2.0	
Level of Publicity	Concealed	-0.3				
	Known	0.0				
refer to paragraph 169	Publicised	0.3				
Accountability	None	0.0				
	Partial	-0.3				
refer to paragraph 175	Comprehensive	-0.6				
					Calculated EAL	

System:
Confidentiality Barrier:
Calculated by:
Date:

This page is intentionally left blank

APPENDIX 5 TO

ANNEX B TO

CHAPTER 6

METHOD OF ANALYSIS USING THE DOMAIN BASED APPROACH

1. The methodology for carrying out an analysis of a system or network proposed by CESG involves the use of a Threat/Access ("Spider") Diagram to replace the network diagrams used in the previous issue of the Standard (as CESG COMPUSEC Memo 10 version 2.2).

2. Since that time, the MOD, via DERA CIS3 and IA(ICS)'s Applied Research Package (ARP) 21.c has independently evolved the Domain Methodology for defining systems and networks, and advice on its use can be obtained from IA(ICS)Impl.

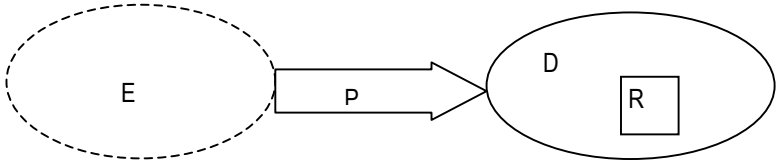
3. Although the methodology does not at present cater for a Threat/Access diagram, it does support the identification of threats within the existing Domain Model notation. Guidance on identification and analysis of these threats is given below.

4. A domain model identifies the physical environments from which people operate computer systems. These contain the potential attackers that may constitute a threat to the data in the system. It also defines domains within the system that represent the logical places where people invoke software to work on their behalf. Membership of a domain provides facilities to reach data and enables members to pose a different threat to the data in the system. For this reason, they may be regarded as distinct groups of potential attackers. Data is held in Repositories that may be reached from one or more domains.

5. As part of the domain model, a set of tables defines the numbers and minimum clearances of members of environments and domains and the maximum protective markings of data handled in domains. The model therefore provides the basic information required to identify threats and analyse them at a high level. In depth analysis of the threats, however requires detailed knowledge of the technical design, configuration and modes of operation of the IT that implements the security requirements expressed in the domain model. Discussion of how this is achieved is beyond the scope of this note.

6. The diagram below illustrates a simple domain model. The data in repository R is reachable from a domain D representing a computer system that may be operated from a physical environment E by entering portal P.

Fig 1. A portal enables some people to enter a domain.



7. In this case, there are at least two groups of potential attackers for the data in R: the members of E who are not members of domain D, and the members of D. The barriers to be considered should therefore:

a) prevent entry to the domain by those who are not members;

b) control access to data in R by members of D, including those who lack the clearances, special access approval or need to reach it.

8. The first of these barriers consists of a single 'logon' measure to counter the threat of non-members attempting to enter the domain. Calculation of the required EAL for this barrier uses the normal calculation for confidentiality. It is based on the characteristics of the environment members as potential attackers and the minimal facilities available to them in attempting to logon.

9. The second barrier may be compromised by several means. Members without the access rights to data may attempt to obtain access to it. Members with access rights to the data may release it either accidentally, or through failure to follow procedures, or because they are traitors. Different measures are required to counter these different causes of compromise. They comprise access control measures, which may include labelling and user-sanctioned release, and accounting measures, which although they do not prevent compromise, can limit the damage caused.

10. For the access control measures, the normal Memo 10 calculation for confidentiality applies, while for the accounting measure, a separate table is used to calculate the required EAL. The potential attackers in this case are all the domain members and the facilities available are all those provided to users in the domain.

11. Access control and accounting measures both depend on identification of the domain member concerned, which is provided by the logon measure. The required EAL for the logon measure is therefore the greater of the levels calculated for each of the barriers that depend on it.

12. In practice, domain models will be more complex than in this example. The members of connected domains must also be included as potential attackers and data handled by these domains must be considered as data under threat. In most cases, the potential attackers will be divided into separate groups according to clearances etc. and the data will be divided into groups according to protective markings.

13. In addition, different types of connection between domains will permit different causes of compromise and will determine the facilities available to potential attackers. Hence further division of groups will be made on the basis of technical factors. While such factors are crucially dependent on the design of the system, the domain model of security requirements can give a good indication of what these might be.

14. In the case of messaging channels between domains which do not carry attachments capable of carrying executables the facilities available are rated as 'low', but if the attachment may carry executable code such as macros, the rating is 'normal'. A connecting repository which is read-only within a domain will reduce the facilities available to other domains, which may therefore be rated as low, whereas for read/write repositories, the rating would be normal.

15. In assessing the different causes of compromise and consequent threat posed by groups of potential attackers to some data, it is necessary to make some assumptions about the facilities provided to users within and between domains, how these facilities will be implemented and the security measures that may be employed. These assumptions may relate to IT and/or procedures and must be recorded with the results of the calculations to which they apply.

This page is intentionally left blank

ANNEX C TO

CHAPTER 6

MOD FUNCTIONALITY REQUIRMENTS FOR COMUNICATIONS AND INFORMATION SYSTEMS

1. **Marginal Assurance Levels** Where the calculated assurance level lies between EAL0.0 and EAL1.5, there is no mandated need to carry out a System Certification, and what CESG refers to as "Health Check", i.e. a combined ESE Verification & LSE / GSE Verification, as laid down at **Chapter 12**, should be performed.

2. For systems constructed from commercial-off-the-shelf (COTS) components, wherever possible "trusted" products should be used in implementing the system to be subjected to the ESE / LSE / GSE Verification, with minimum functionality and degree of "trust" as laid down in the following table :

Function	CL4	CL3	CL2	CL1
Boot Protection	(Optional)		FTA	
Media Protection	(Physical protection)		CAPS File Encryption	CAPS Disk encryption
Low Level ID&A (BIOS Passwords)	COTS			
User Level ID&A (Passwords)	See **Chapter 6 Annex A**			
User Level Access Controls (File System or Encryption)	(Optional)		FTA	
Administration Privilege Access Controls	(Optional)		FTA	
Accounting and Audit	COTS			
Integrity –Workstation Media Authentication Guard (WMAG)	(Optional)		FTA	
Integrity – Anti Virus Software (AVS)	MOD recommended product, as defined in annual DIAN			
Integrity – control of executables	(Optional)		FTA	

Backup Software	COTS	
Network protection – protocol control ("FireWall")	COTS	FTA
Network protection – Secure Remote Access	As required by **Chapter 23**	CAPS
WAN encryption	Optional	CAPS

3. Where encryption is mandated, this is an additional precaution to any requirement arising from the protective marking level of the system. CAPS stands for the CESG Assisted Product Scheme.

ANNEX D TO CHAPTER 6

ASSURANCE ACTIVITY FEEDBACK FORM

RESTRICTED – COMMERCIAL
(when completed)

Project / System Summary			
Name		**Reference(s)**	
Date Started		**Date Completed**	
Overview			
Project Office Contact			
Name	**Position**	**Telephone**	**Location**
Assurance Activity Summary			
System Element	**Assurance Type**	**Level Achieved**	**Comments**
Comments on Assurance Activities			
Meeting Requirements			
Timescales			
Costs			
Overall Satisfaction			

NOTES

Where elements are COTS or GOTS products that have been included as part of a system, these should be itemised separately.

(when completed)
RESTRICTED – COMMERCIAL

This page is intentionally left blank

ANNEX E TO

CHAPTER 6

PROTECTIVE MONITORING INTERIM GUIDANCE

Guidance For Using This Document

1. The purpose of this document is to enable system owners/administrators to develop an appropriate monitoring policy for their system based upon knowledge of the potential threats to their systems integrity, confidentiality and/or availability.

2. Section III describes the potential threats to a system in a generic manner. A user of this document should read this section and determine which threats are of greatest concern to their system.

3. Section IV briefly describes the various objectives that should be met in order to cover the different threats detailed in Section III. The user should familiarise themselves with the objectives that are required to meet the threats that are of particular concern to their system.

4. The descriptions used in Sections III and IV are generic and not specific to any service that may be utilised by a network user. Section V addresses the security requirements that underpin the objectives of Section IV, and it is here where the descriptions become more specific.

5. In order to gain full value from Section V the user should consider what services are provided on their network, and whether any could pose a potential risk. This will determine which of the security requirements will need to be implemented.

6. This document does not state how the security requirements should be implemented. It is up to the individual user to determine whether, in their network, the requirement should be met by a technical solution or by a procedural measure.

Introduction

PURPOSE

7. This document is intended to enable government departments to develop policies for the protective monitoring of their network in line with current regulations and government policies.

8. This document provides interim guidance only. CESG's aim is to issue a formal memorandum by the end of 2001.

SCOPE

9. This document describes the perceived threats relevant to a system that has connections with less assured domains. It then defines a set of security objectives that such a system should meet, and finally defines a set of detailed security requirements that meet the objectives.

10. The content of this document is based upon CESG's current understanding of technologies, threat, vulnerabilities, and departmental requirements.

11. This policy is also intended to help Departments ensure compliance with the Lawful Business Practice Regulations and related telecommunications data protection legislation.

DEFINITIONS

12. Compusec Memo 1: "Audit":

a. An independent review and examination of system records and activities in order to test for the adequacy of system security measures, to identify the degree of conformance with established security policy and operational procedures and to recommend any indicated changes in measures, policy and/or procedures.

b. Monitoring to detect and warn of events which might threaten security.

Note: The term "security audit" may be used to avoid ambiguity.

Background

INTRODUCTION

13. Protective monitoring should form part of a suite of countermeasures (including e.g. virus checkers and firewalls), designed to counter the threats faced by systems which are connected to public networks such as the Internet. The objectives of the monitoring would be threefold.

a. Firstly it should provide a mechanism whereby user compliance with a departmental security policy could be monitored.

b. Secondly it should reduce the risk from attack (internal or external) to the system being monitored, and to other departments to which it is connected

c. Finally it should provide records to support appropriate incident reporting, investigation, and response.

14. Monitoring can be carried out at system or Intranet level, where an Intranet is a system or systems such as the GSI. System monitoring should be primarily concerned with ensuring safe user behaviour and identifying anomalous user and network activity, ie it should endeavour to identify activities likely to compromise system information. Intranet monitoring should be concerned with identifying events that occur across a number of systems and which may not be visible at the system level.

15. Whilst it is strongly recommended that departments monitor all IT systems that that have connections to public networks, departments should also consider applying similar techniques to systems that have no external connectivity to help maintain the integrity, confidentiality and availability of system services.

16. Monitoring may, at the department's discretion, also be used for other lawful purposes. It could, for example, detect abusive or offensive material or improper use of official assets. However, departments should be aware of the requirements of the data protection regulations detailed in Section B.

COMPLIANCE WITH HRA AND OTHER LEGISLATION

17. Protective monitoring policy must be compliant with the following legislation:

The Human Rights Act 1998
The Data Protection Act 1998
The Regulation of Investigatory Powers Act 2000
The Lawful Business Practice Regulations 2000

18. The Data Protection Commissioner will be publishing an Employment Code of Practice in 2001, which also deals with monitoring. The consultation draft stressed that monitoring should not intrude unnecessarily on employees' privacy and autonomy. The Commission's Code is an authoritative statement on the subject and should be closely followed.

USER NOTIFICATION

19. *The Lawful Business Practice Regulations* permit the monitoring of IT systems by managers for specified purposes, including in the interests of national security, to prevent or detect crime and to secure the effective operation of the system. But they stipulate that 'reasonable efforts' must be made to notify all users of the system of the monitoring. Cabinet Office Security Division have advised that 'reasonable efforts' might include circular notices, pop-up messages, information within e-mail banners/disclaimers, notices on Intranet home pages and statements in staff handbooks/employment terms.

20. Information collected during monitoring should not be used for purposes other than those for which it was introduced, and about which users were notified, unless it reveals criminal activity or gross misconduct.

Threats

INTRODUCTION

21. This section documents the currently known threats that are relevant to any department with a system connected to public networks.

SPECIFIC THREATS

T1 *Accidental export of sensitive data to an inappropriate system.* Examples: A user wrongly addresses an e-mail or uses a distribution list which contains recipients outside the government system; a user accidentally modifies some aspect of the system, which results in the export of data; an administrator incorrectly configures a system component such as a Domain Name Server, which results in information being routed outside the government system; a software or hardware failure results in the misrouting of data outside the system.

T2 *Deliberate export of sensitive data to an inappropriate system*
Examples: a disgruntled employee consciously releases sensitive information to entities not permitted access; or modifies an element of the system with the net result that information is released; a service, such as Web-based disk storage, utilised by a user as a convenient means of storing department information to allow access from home.

T3 *Exploitation of an allowed service to export sensitive data to an inappropriate system* (an allowed service is one that is permitted by the local security policy and supported at the system boundary).
Examples: an external entity may use an allowed service to introduce malicious code into a system. This code may affect the integrity or availability of the system, or may use the same or similar allowed service to export sensitive information from the system. The code could be introduced through other means (e.g. floppy disk or CD) with the same outcome.

T4 *Exploitation of a disallowed service to export sensitive data to an inappropriate system* (a disallowed service is one that is not permitted by the local security policy and should not be supported at the system boundary).
Examples: an external agent may discover a configuration error, implementation flaw, or hardware failure in a boundary component such as a firewall, which can be used to introduce malicious code or directly extract sensitive information from the system.

T5 *Denial of responsibility for an action*
Example: a user may deny carrying out an action that led directly or indirectly to the export of sensitive information to an inappropriate domain.

T6 *Modification of evidence*
Example: an entity may modify system record to hide evidence of illegal activity.

Assumptions

INTRODUCTION

22. It has already been stated that defensive monitoring is only one of a number of countermeasures that should be employed. It is assumed that these countermeasures will be applied to a system being subjected to defensive monitoring.

SECURITY ASSUMPTIONS

A1 The configuration of key components will be tested in accordance with a documented test plan. The test plan should include all foreseeable eventualities. For example, when a virus enters a system, mail servers are often shutdown in order to contain its spread. This will cause servers outside the system to attempt to use alternative routes that are inappropriate for the sensitivity of the data. Therefore in this case the test plan must ensure that alternative routing strategies that would be employed as a result of system degradation have been tested.

A2 The system will be designed to minimise the risk that a component failure will compromise the confidentiality, integrity or availability of a system, ie systems should be resilient to technical failure.

A3 Users will be educated to understand the implications of, and their responsibility for, their actions. They will be notified that monitoring/recording may take place, so that there can be no expectation of privacy.

A4 A clear "acceptable use" policy will be declared to users – and will be formally accepted by users before they are allowed access to system services and resources. Users will be periodically reminded of what constitutes acceptable use, and immediately following any change in the usage policy.

A5 Disciplinary procedures for breaches of the 'acceptable use' policy will be published and rigorously enforced.

A6 Administrators will be trusted not to compromise a system intentionally, and will be educated to understand the implications of their actions.

A7 A department will implement appropriate measures to prevent malicious code or code which could be put to malicious use (trojan, virus, compilers or standard hacking tools) from entering a system.

A8 Systems will only support services at their boundary that are supported by a clearly justified business case. All others should be blocked by a suitably approved firewall.

A9 All existing barriers will have been subjected to a risk assessment in accordance with HMG Infosec Standards, and implemented as required by those standards.

Security Policy Objectives

INTRODUCTION

23. This section defines a number of objectives that counter the threats identified in section four.

OBJECTIVES

O1 **Policy** - A local auditing policy shall be produced.

O2 **Information Release** - Auditing shall look for evidence that sensitive information is being released from the system by electronic means.

O3 **Potential Release** - Auditing shall look for evidence that users are behaving in a manner that could result in the release of sensitive information.

O4 **Allowed Service** - Auditing shall look for evidence that an allowed service is being used to compromise the system.

O5 **Suspicious Activity** - Auditing shall look for evidence of suspicious activity.

OBJECTIVES, ASSUMPTIONS AND THREATS

24. The following table demonstrates how the objectives and assumptions are intended to counter the identified threats. This table should be used to ensure a threat has been sufficiently countered.

	T1	T2	T3	T4	T5	T6
A1	x			x		
A2	x					
A3	x	x				
A4		x				
A5		x				
A6		x				
A7			x			
A8			x	x		
A9				x		
O1	x	x	x	x	x	x
O2	x	x	x	x		
O3	x	x	x			
O4		x	x			
O5	x	x	x	x		x

Security Requirements

INTRODUCTION

25. This section defines the security requirements that should be met in order to meet the objectives defined in the previous section.

26. The specific security requirements that will need to be included in departmental security policies will depend upon the threats that are relevant to the system and the services supported.

POLICY

SR1 An auditing policy shall define the following:

SR1_1 The threats relevant to the system.

SR1_2 The objectives of the policy relevant to the threats.

SR1_3 The security requirements relevant to the objectives.

SR1_4 The appropriate roles and responsibilities for the audit process (Note wherever possible the roles of System Administrator and System Security Officer should not be carried out by the same person).

SR1_5 The time within which an administrator must become aware of an event.

SR1_6 The procedure to be followed by the administrator in response to an event.

SR1_7 The events that must be investigated.

SR1_8 The mechanism by which time shall be synchronised across the system.

SR2. The following information shall be recorded by appropriate components within the system.

SR2_1 For e-mail related events this should include: subject, originating user, recipient(s), time of origination, information relating to the resolution of addresses, the time at which it was exported, and the nature of the event.

SR2_2 For web related events this should include: originating IP address and user name, destination IP address, destination URL, information relating to the resolution of addresses, transaction time, nature of event and the number of bytes being sent and received.

SR2_3 For network related events this should include: source and destination addresses, ports and the nature of the event.

SR2_4 For host-based activities, this should include: source and destination addresses, ports, the user name, any information used to resolve addresses, and the nature of the event.

SR2_5 All messages leaving the system shall be archived for a period determined by the department. (But note the Data Commissioners' Code in this context).

INFORMATION RELEASE

SR3 Procedures and/or processes shall be implemented to identify the following events.

SR3_1 Outbound e-mail containing one or more keywords which may indicate it is sensitive and should not be released. The exact keywords that indicate sensitivity will depend on local conditions.

SR3_2 Outbound HTML traffic containing one or more keywords which may indicate it is sensitive and should not be released. The exact keywords that indicate sensitivity will depend on local conditions.

SR3_3 Procedures shall be implemented to manually check, at random, the content of e-mails to ensure they do not contain sensitive material.

POTENTIAL RELEASE

SR4 Procedures and/or processes shall be implemented to identify the following events.

SR4_1 Interactions with web site supporting the following types of service: Web-based e-mail, virtual disking and on-line vulnerability scanner and chat.

SR4_2 Interactions with web sites dealing with the following subjects: hacking, viruses, trojans.

SR4_3 Use of an e-mail auto-forwarding mechanism to an external address.

ALLOWED SERVICE

SR5 Procedures and/or processes shall be implemented to identify the following events.

SR5_1 Use of encryption to protect Web transactions and e-mails.

SR5_2 Web interactions involving active code (ActiveX, Java, etc).

SUSPICIOUS ACTIVITY

SR6 Procedures and/or processes shall be implemented to identify the following events.

SR6_1 Attempted use of anonymous or default accounts within the following components: router, firewall, web/mail proxy and mail server.

SR6_2 Failed attempts to gain access to a component service.

SR6_3 Attempted exploitation of known component vulnerabilities.

SR6_4 Use of network mapping mechanisms such as ‘ping’ and ‘port scan’.

SR6_5 Attempted use of unsupported services within the following components:

SR6_6 Unusual traffic patterns.

SR6_7 Unexpected gaps within the logs within the following components: routers, firewalls, web/mail proxies and mail servers.

OBJECTIVES VERSUS REQUIREMENTS

	O1	O2	O3	O4	O5
SR1	x				
SR2	x				
SR3		x			
SR4			x		
SR5				x	
SR6					x

MALICIOUS SOFTWARE

This page intentionally left blank.

CHAPTER 7

MALICIOUS SOFTWARE

Introduction

0701. Malicious Software is a general term covering several types of software code introduced into a system to perform tasks that are not part of the system's designed functionality. Malicious software is intended to compromise a Communications and Information Systems by breaking its confidentiality, corrupting its integrity or affecting its availability. It is not to be confused with unexpected functions due to errors in software, mis-keying, or the misuse of operating system commands.

0702. Some forms of malicious software, especially viruses, present a real risk to MOD CIS. Viruses, in terms of numbers of security incidents, represent the biggest threat to MOD CIS. Relatively simple countermeasures can minimise the risks. A key countermeasure is high user awareness of the problem. Anti-virus software (AVS) must be installed on all MOD CIS. It is also essential to ensure that latest version of the AVS is installed.

0703. Variants of malicious types appear almost on a daily basis. In most cases the visible impact on your system will be different though the general advice contained in this Chapter will always be relevant. CESG Infosec Memorandum No. 12 gives additional information on dealing with the different types of malicious software.

Types of Malicious Software

0704. The boundaries between different types of malicious software are not always clear-cut but they generally fall into one or more of the following:

a. **Viruses**. These are so called because they attach to healthy programs and replicate themselves, thus infecting other programs and systems. The primary target for viruses is the PC operating system but all major operating systems have been targeted though to a lesser extent. Viruses are, by far, the most common type of malicious software and a whole industry has been built up to combat them

b. **Trojan Horses**. A Trojan horse is a program that pretends to do one thing while performing another, unwanted action. Any executable file sent as an attachment could contain a Trojan. The most well known Trojan is where the 'Login' screen is mimicked, enabling usernames and passwords to be stolen

c. **Logic bombs**. A Logic Bomb is a malicious program routine triggered by a specific event or situation. The triggering event could be a date (eg Friday

13th) or a change made to a database record (eg a change to Joe Bloggs' employment status) or any other event that can be recognised by software.

d. **Worms**. Worms, like viruses, replicate themselves but they do not attach to specific programs. A variant is where the original program makes copies of itself but retains control over its 'offspring'. The primary target for worms is networked systems.

e. **Mobile Codes**. Mobile codes can be used maliciously. Mobile codes are meta-codes, which are designed to be executable on multiple platforms or architecture by use of an intermediary interpreter or virtual machine. Examples of mobile code are Java, Javascript, ActiveX, COBRA and software agents.

Effects

0705. The actual damage done to the security of the system under attack depends on the action triggered. This action is called 'the payload' and can vary from benign or no action to catastrophic action. In general, malicious software attacks system availability and data integrity by corrupting files on the system. Attacks against the confidentiality of data on the system are less common. The most obvious attack on confidentiality is the clandestine capturing of usernames and passwords for use in subsequent hacking attacks.

Threat

0706. Malicious software can originate from many sources such as disaffected staff, foreign intelligence services, investigative journalists or terrorists. However, in practice, the vast majority of malicious software attacks originate from delinquent enthusiasts who are unlikely to gain from the inconvenience caused apart from a certain amount of notoriety. There are exceptions to this.

Vulnerabilities

0707. In order to be effective, a malicious software attack has to gain access to the system in some way. Viruses can be propagated in a number of ways. Any medium that can store or transmit data can carry a virus including: diskettes, CD-ROMs, network communication lines, telephone/modem lines, disk fax machines and e-mail attachments. The most common sources of risk are described below.

a. **Software**. Pirated software, engineering diagnostic software, free software given away with magazines, shareware and even shrink-wrapped commercial software from reputable sources have all been responsible for spreading viruses. The only way to provide your system with adequate protection is to trust no one; almost all viruses are spread unintentionally. Check everything for viruses before placing your system at risk.

b. **Internet**. The Internet is a popular source of viruses and all files downloaded from e-mail, bulletin boards, web-pages or any other Internet source should be treated with suspicion until they have been checked.

c. **Home Computers**. Carrying out official work on home computers is becoming more common; unfortunately, the majority of home users do not practise safe computing and can bring viruses into the office. The advent of macro-viruses has dramatically increased the risk of infection from this source. Disks must be checked every time they have been used outside the office.

d. **E-mail**. E-mail messages themselves may carry viruses but more commonly attachments are used. Macro-viruses are the most common forms spread in this way. An attachment should not be opened until it has been scanned.

e. **Deliberate Infection by a User or Hacker**. The vast majority of virus incidents are accidental but the deliberate introduction of a virus into a specific system is possible and may be attractive to some.

0708. A number of ways of gaining access to a system, for the purpose of delivering malicious software, are described below:

a. Access during software development by authorized programmers provides opportunities for building in Trojan Horses and Logic Bombs. This is unlikely in proprietary products not aimed specifically at the defence market, but 'time bombs' designed to ensure licence payments are not unknown. Risks to bespoke software can be reduced by the use of quality assurance and appropriate personnel security clearances.

b. Access via communication links. Systems accessible to public communications networks are extremely vulnerable to hacking and no such connection may be made without authority from the appropriate accreditor. Direct connection to a public network is easily avoided by the system administrator but considerable care should be taken to ensure that onward connection is not made via another system. This includes remote diagnostic facilities.

c. Access via a user terminal. This could be either a keyboard or other software loading point such as a disk drive. A user can be an end user, systems user or programmer, each presents different risks. In general, stand-alone and small networked systems use DOS, Windows 3.x, 95, 98, 2000 or NT which allow easy access to all parts of the operating system making them vulnerable to attack.

Vulnerability Classes

0709. The Joint Security Co-ordination Centre (JSyCC), as described at Chapter 2, is responsible for maintaining a central source of Vulnerability and Threat information for all aspects of CIS security, promulgating Vulnerability Warning Notices (VWN) as necessary.

0710. Vulnerability Warning Notices (VWN) in respect of Malicious Software will consist of Alerts and Rectification Directives, as discussed at Chapter 2, which will be issued on the basis of Vulnerability Classes, as defined below:

Vulnerability Class	**Risk**	**Impact**
A	Very High	High
B	High	
C	Significant	Medium
D	Moderate	
E	Low	Low
F	Negligible	

0711. Using this categorisation the System Operating Authority (SOA) action required can be determined:

Vulnerability Class	**Criticality Level**			
	CL4	**CL3**	**CL2**	**CL1**
A and B	As laid down in Rectification Directive			
C	Weekly	Daily	Daily	Immediate
D	Weekly	Weekly	Daily	Daily
E	Monthly	Weekly	Weekly	Daily
F	Monthly	Monthly	Weekly	Weekly

Countermeasures

0712. Countermeasures, which should be recorded in the SPD/SyOPs, are available to reduce these risks to an acceptable level. Only authorized and licensed software and media are to be used on Defence IT systems. Controls can be procedural but this has been found to be unreliable. A better approach is to reinforce this with Workstation Media Authorization Guards (WMAG). Annex A gives more details about WMAG. Specific anti-virus measures are dealt with in more detail below in paras 0721 to 0728.

Software Development

0713. There are two main ways in which software development and amendment takes place: When an upgrade of the operating system or application programs is offered by a computer manufacturer, or where software programs are written by suitably qualified "In-House" personnel, to enhance or develop applications and utilities. The following

security measures are to apply to software amendment, upgrade and development:

a. **Assurance.** Software enforcing security functionality may require evaluating and certification in accordance with current national standards. This process effectively defines the quality assurance level required in the preparation of such software.

b. **Commercial Software.** All system software changes must be authorized through a formal change control procedure. In certain circumstances, where a software amendment is received from a software manufacturer or MOD Software Bureau, the two-person rule may need to be applied when the amendment is loaded onto the system. This is to ensure no unauthorized modification and/or tampering can take place from the time it is received from the supplier until the time it is loaded into the system.

c. **In House Development Software.** Where software programs and/or amendments are carried out "In-House" by suitable qualified staff, the following measures are to be enforced:

(1) A system of quality inspection is to be established to ensure that no unauthorized modification and/or amendments have been made to the software.

(2) The amendment and change is to be fully documented and hard copy of the software code is to be retained on file.

(3) The software is to be thoroughly tested on an independent PC or system before loading onto the operational/live system.

(4) The two-person rule is to be strictly adhered to when loading the software onto the operational/live system to prevent unauthorized modification and tampering before the loading takes place.

(5) The software amendment or change must be authorized through a formal change control procedure.

Viruses

0714. Most viruses are designed to attack systems running the most popular operating systems. To date these are DOS, Microsoft Windows 3.x, 95, 98, 2000 and NT. Viruses have been written for other operating systems such as Linux and the Apple Macintosh environment but these make up a fraction of the overall virus population

0715. Viruses come in a variety of forms using different techniques to both hide and

propagate. Initially, viruses could only spread via the Boot Sector of a disk or with an executable program file. The macro language facility in Microsoft Office products, especially Microsoft Word, provides the environment for a new generation of virus writers. The development of powerful macro languages has blurred the boundary between data and programs making it possible to propagate viruses via wordprocessing documents and spreadsheets.

0716. Macro-Viruses now pose the greatest threat to systems, as they are much more likely to be passed from user to user, either via diskette or e-mail. This technique also allows macro viruses to cross to different operating systems because an infected Word document created on a Windows machine might run quite happily on an Apple Macintosh running Word.

0717. The popularity of Microsoft Word has led to the majority of macro viruses to date being written for this, and other, Microsoft Office products. Any Word document file, unless it is in RTF format, could potentially contain a virus. Staff should not assume the macro virus problem only exists for Microsoft - any product that gains popularity and has a facility to execute user statements is liable to be misused by the virus writers.

0718. Any form of executable file or object is vulnerable to virus infection. Once activated the virus payload may attack any file stored within the system, or any system within a network. Systems are particularly vulnerable in working areas where access and the circulation of floppy disks are uncontrolled. E-mail attachments are now the primary method for transporting infected objects.

0719. Actual infection of a host computer occurs when the virus code is executed. Viruses are designed so that the act of executing them is triggered without the knowledge or consent of the user, when a normal process is carried out.

0720. There are a number of ways of detecting viruses; none of them are perfect. Viruses can be identified directly by their form or signature, by their actions or by changes made to previously uninfected files. It is these techniques, along with strong procedures, that allow the threat from viruses to be combated. Annex B gives details of techniques of virus detection. Annex C gives details of defensive techniques against viruses.

Anti-Virus Software

0721. The use of anti-virus scanners is fundamental to effective anti-virus strategy and forms a key component of MOD policy. A wide range of anti-virus software (AVS) is available to scan systems, exchangeable media, and network traffic for known viruses. AVS must be installed on all MOD CIS and kept up to date. Experience has shown these to be generally effective.

0722. There are however a considerable number of scanners available with no formal evaluation or readily available guidance on their relative effectiveness. MOD commissioned a DSTL study of open source publications with the aim of producing a list of trustworthy market leading of commercial off the self (COTS) AVSs.

0723. The list is published in Defence Information Assurance Notice No.5, which is distributed to PSyA staff. The scanners listed have given good test results in recent open publications and provide a market leading measure of protection against viruses. The list will be reviewed regularly and updated as required.

There are 3 fundamental placements possible for AVS:

a. At system boundaries ;

b. On all hosts;

c. On workstations.

0724. The nature of the "boundary" placement will depend on the system architecture implemented, and could be using a WMAG on a small LAN or an e-mail content checker on a large network.

0725. Where information transfer is by media transfer, all incoming and exported media is to be checked for viruses and the systems themselves checked on a regular basis. This is particularly important where systems exchange data by disk transfer, including diskfax interconnections.

0726. The following table gives an indication as to where the AVS should be placed:

Operating Mode	**Criticality Level**			
	CL4	**CL3**	**CL2**	**CL1**
MLS	All Hosts	All hosts & Boundaries	All hosts & Boundaries	All hosts & Boundaries
Compartmented	All Hosts	All Hosts	All hosts & Boundaries	All hosts & Boundaries
System High	Workstations	Workstations	All Hosts	All hosts & Boundaries
Dedicated	Workstations	Workstations	Workstations	All Hosts

0727. Before entering into a contract for AVS, the required frequency for availability of updates must be ascertained, based on the Criticality Levels of the systems and the ratings of malicious code:

Vulnerability Class	**Criticality Level**			
	CL4	**CL3**	**CL2**	**CL1**
A and B	Within 1 week	Within 1 day		Within 12 hours
C to F	Within 1 month			Within 1 week

0728. For critical systems consideration should be given to using two different AVS products in tandem. AVS products should always be kept current.

Impact of Cryptography

0729. Where Baseline Grade (BG) cryptography is being used to provide desktop to desktop encryption between end user computer systems, the Accreditor may require that encryption keys be lodged at any MOD controlled Secure Managed Interface (SMI), as defined at **Chapter 15,** that is transitted to facilitate checks for Malicious Software.

Training and Contingency Plans

0730. Training of all users in measures against malicious software is critical; otherwise protective procedures will not be followed. Helpdesk staff should also be trained in recognising virus infections and should be familiar with reporting procedures. It is also essential that effective contingency plans are in place to recover systems from virus attacks and this implies trained personnel as well as suitable software.

Management Controls

0731. Most network operating systems employ security features which if applied correctly will provide adequate file protection. Any file or directory on the network that the user can modify is at risk from a virus. The system administrator should adhere to the following rules when setting permissions for files/directories on the network:

a. All executable files and shared templates on the network should be put into a read-only directory.

b. Each user should have their own private home directory on the network. Other users may be allowed to read from but not write to these home directories. If a user's workstation becomes infected the same user's home directory on the network may also become infected but the rest of the network will be safe.

c. There is often a requirement for shared directories on the network.

These allow, for example, for documents to be created and modified by more than one user. If one user's workstation becomes infected the shared directory may become infected. If a second uninfected user workstation then accesses files on the shared directory this too may become infected. Each time a file is accessed from the shared directory it should be treated with caution and checked with anti-virus software prior to opening.

0732. For large systems and networks the system security officer, or an appropriately security trained member of staff, should be identified as the focal point for the reporting of virus infections. This role should be defined, together with an agreed scope of authority, in the Security Policy Documentation. This member of staff should be familiar with the escalation procedures in event of a large-scale virus infection. These escalation procedures should cover actions to be taken with regard to connected systems and reporting procedures to higher MOD authorities. Incident Handling is covered in **Chapter 11**.

0733. Large systems and networks should have documented procedures on managing incidents, in the form of an Incident Response Plan (IRP) as defined at **Chapter 3**. This should include details as to how levels of degradation are to be managed, if it is required for operational reasons. For networks and interconnected systems it may be necessary to have a form of Service Level Agreement to cover circumstances, which could include whether to:

a. keep the system running and manage in conjunction with the AVS vendor;

b. sever interconnections with other systems;

c. take the system down.

User Action in the Event of a Virus Infection

0734. Users should be familiar with the actions required by the SyOPs in the event of a virus infection. The actions and disinfection procedures will vary between systems and according to the stage of the infection. If in doubt and a virus attack is suspected the following actions must be taken:

a. STOP USING THE WORKSTATION AT ONCE.

b. Do not switch off or re-boot the system until given permission to do so by local Security staff.

c. Inform the System Manager, SSO and ITSO immediately. Preservation of evidence may be necessary. Do not remove or destroy media. Statements will need to be recorded if it is considered an offence has been committed.

d. Locate and isolate all disks and other I/O media, which may have been used on an infected workstation.

0735. The Security Staff will:

a. Identify and isolate any workstation, which may have been infected.

b. Identify and warn any users that may have been sent infected files.

Recovery

0736. Once the PSyA is satisfied that an investigation will not be compromised they may authorize disinfection and, where required, data recovery procedures. Virus scanning and eradication of viruses from suspect workstations and disks is only to be carried out by personnel specifically authorized to do so by PSyA.

Reporting and Investigation

0737. All malicious software incidents are to be reported initially using the format laid down in Annex A to Chapter 11, then, when resolved to the Unified Incident Reporting and Alert Scheme as described in Chapter 11. It is essential that an investigation is carried out so that the source of the malicious software can be established and action taken to limit the spread of infection and minimize the chance of recurrence. The investigation should be initiated by PSyA in accordance with their own procedures.

ANNEX A TO CHAPTER 7

WORKSTATION MEDIA AUTHORIZATION GUARD (WMAG)

PREVIOUSLY KNOWN AS FLEXIBLE DISC AUTHORIZATION GUARD (FDAG)

1. Systems which prevent unauthorized floppy disks being used on the PC, significantly reduce the opportunity for viruses to be introduced. However, unless authorization is always preceded by a thorough virus scan, preferably by more than one scanning product, they provide no specific defence against the virus itself.

2. WMAG are proactive in that they aim to prevent any situation where a virus can infect a computer system through a floppy drive. They work on the principle that once the guard system is loaded on a PC, only authorized floppy disks can be used. Whether or not the individual PC is granted the right to authorize software is decided when the system is loaded. WMAG provide a mixture of software and hardware control.

3. Usually one PC would be nominated as a 'gateway' (sheepdip) PC for a group of PCs. For safety, the gateway should be a standalone PC, at least while it is being used in the gateway mode. It is then used to scan all floppy disks to ensure they are free of infection. Most WMAG type products come 'bundled' with a virus scanner. It is generally agreed that it would be sensible to use a second virus scanner to give some additional protection. Once the disk is declared 'clean', the WMAG then adds an electronic signature to the disk. This signature contains a checksum which is related to the contents of the disk. It is this signature that is required by every other PC to prove that it has been authorized. Some WMAG systems use this mechanism to prevent the disk from being used on other PCs, which have not been loaded with the WMAG. Some WMAG systems permit the disk to be used outside the group, but if the disk is written to by any device which does not have the WMAG loaded, the checksum will become invalidated. Subsequently, when the disk is loaded onto a WMAG PC, the signature is verified before any access is permitted. Any disk which has been used outside of the WMAG group would be required to be scanned and reauthorized by the gateway PC.

4. Some WMAG have additional utilities to monitor all processor activity and then to prevent and report any actions which have been designated by the user as illegal, such as an unauthorised write access to elsewhere on the disk. This helps identify any virus which has not been caught by the gateway scan or has been introduced into the PC through the communications port from a modem.

5. The main advantages of the WMAG system are that:

a. Only authorized floppy disks can be used with the PC. This not only reduces the risk of malicious software, but also the use of pirated software and generally any unofficial software.

b. Only those PCs designated as gateways need have virus scanning software bought for them. This reduces the overall cost and also the upgrading effort required every time an update for the scanner is produced (this can be every month). Of course, in some circumstances, each stand alone PC can be designated as its own gateway and thus authorize its own floppy disks. However this detracts from the additional control which this system offers and should be discouraged unless required for local operational/justified reasons.

6. The only disadvantage of using WMAG is the additional cost. However WMAG type systems are typically significantly cheaper than virus scanners. The cost of any additional virus scanner would be limited to the number of gateway machines.

ANNEX B TO CHAPTER 7

TECHNIQUES OF VIRUS DETECTION

Categories of Virus Protection Products

1. Virus protection products can be divided into three broad categories: 'On demand', 'On access' and activity monitoring. 'On demand' products require the user to initiate virus detection by starting the anti-virus software manually. This is the most common way of using scanners and is ideal for providing a controlled anti-virus boundary for an organization. It is only necessary to install such software on a small number of quarantine "sheep dip" PCs to provide a measure of protection for all the organization's PCs. 'On access' products check files automatically whenever they are to be accessed. To be effective, this software must be installed on all the systems to be protected. Activity monitoring software does not detect viruses, as such, but detects and blocks suspicious activity. To be effective, this software must be installed and active on all systems to be protected. Anti-virus software must be upgraded on a regular basis and kept current.

Detection by Virus Signature

2. Each virus has a form that can be recognised by appropriate software provided it is a known virus. This is the basis of the best known type of anti-virus software - virus scanners.

a. Advantages.

(1) The input medium can be scanned for known viruses before any files are loaded or copied onto the system's hard disk(s).

(2) Companion software can normally locate and remove the virus.

(3) A single PC can act as a guard for all other systems by scanning all incoming disks.

b. Disadvantages.

(1) Only viruses known to the scanner will be detected. As new viruses are constantly being created, often by modifying old viruses,

there is always the risk of an unknown virus slipping through undetected.

(2) False detections can occur when part of a valid file is mistaken for a virus.

(3) Compressed and/or encrypted files may thwart the scanner.

(4) Virus scanners must be continually upgraded to take account of new viruses.

(5) Polymorphic (multi-shaped) viruses are particularly difficult to detect as they can change their signature at each replication.

Detection by Virus Activity

3. Viruses can be detected by monitoring the system for 'suspicious' actions. Virus protection software is available that will detect and intercept suspicious actions before any harm can be done.

a. Advantages. Unknown viruses can be detected and harmful actions can be prevented.

b. Disadvantages.

(1) Detects viruses only after they become active, however, if the virus is not allowed to perform any damaging action this may not be considered a disadvantage.

(2) The anti-virus software must be installed and running on all PCs at all times to monitor program activity. Apart from the cost, the presence of such a program will affect system performance.

(3) Legitimate programs may initiate 'suspicious' actions during normal running giving false detections. Most anti-virus programs of this type allow the user to identify 'privileged' programs that are allowed to use specific 'illegal' methods. This can be complex to set up, especially on a large number of PCs, and provides a potential loophole for a virus to exploit.

Detection of File Changes (Checksumming)

4. Viruses that attach themselves to programs will make changes that are detectable. In its most primitive form the program file will become slightly longer but it is possible for

a virus to overcome this. More sophisticated detection methods introduce some sort of 'digital signature' calculated from the original file contents. If the file is infected its signature will be different, making the infection apparent.

a. Advantages.

(1) Can detect unknown viruses.

(2) Has little effect on performance, as the file checking process is only active while a program is being loaded for running.

b. Disadvantages.

(1) Must be installed on all systems.

(2) Will not detect viruses that were already present when the initial file signature was calculated.

(3) Depends on the files it is monitoring being relatively static. This makes the technique unsuitable for guarding against Macro-Viruses.

Heuristic Scanning

5. Although the name implies a learning process, in practice, most software that uses this technique checks files for the potential of 'virus type' activity. This is normally done by disassembling the program code to detect 'suspicious' functions. In essence, it is an activity monitor, which works prior to the virus becoming active.

a. Advantages.

(1) Prevents damaging activity before the virus can execute.

(2) Can detect unknown viruses.

(3) No significant performance implications.

(4) A single PC can act as a guard for all other systems by scanning all incoming disks.

b. Disadvantages.

(1) Can generate many false alarms.

(2) Has been unreliable in the past but this technique is improving and may become the best defence against Macro-Viruses.

This page intentionally left blank.

ANNEX C TO CHAPTER 7

DEFENSIVE TECHNIQUES AGAINST VIRUSES

Introduction

1. An effective defence against viruses can only be provided by using a combination of defensive techniques and anti-virus software products. Security can also be considerably enhanced by effective configuration management. In general, this is easier to achieve with a networked system of PCs controlled by a network manager than with standalone PCs.

Configuration Management

2. Configuration Management (CM) is normally associated with large systems, however, there is considerable advantage to applying it to standalone PCs and small systems to ensure that only authorized software is installed. If CM is introduced and enforced, only authorized software can be installed, significantly reducing the probability of it being infected in the first place and ensuring that it is properly virus checked before installation. It should be noted that the use of unlicensed software is an offence under the 1988 Computer Copyright Acts and the use of licensed software used for a purpose other than that authorized by a user's organization is also an offence under the Computer Misuse Act see Chapter 1.

Back-ups

3. If a system is subjected to a virus attack the only effective means of recovering may be to recover the files from backed-up material. The key to any recovery programme is good backup procedures; accordingly, procedures for regularly backing up data must be identified in system SyOPs.

Prevention of Boot Sector Viruses

4. A PC's vulnerability to boot sector viruses can be reduced significantly by resetting its system default settings in the Basic Input/Output System (BIOS) to boot directly from the 'C' drive instead of looking at the 'A' drive first.

Boundary Protection - Disks

5. An organization can protect itself very effectively from disk borne viruses by setting up a 'Boundary Protection Facility'. Boundary protection is implemented by ensuring that all input media are subjected to virus checking and cleaning on specifically designated "sheep dip" PC(s) before any files can be copied to the organization's working PCs. It is recommended that the "sheep dip" PC(s) utilize both a virus signature scanner and an heuristic scanner (often included in the same package). If effective boundary controls are introduced, disks can be exchanged within the organization with minimum risk of viruses being propagated. Boundary control can be enforced by using disk authorization software which makes it impossible for non-authorized disks to be read by PCs within the boundary.

Boundary Protection - Electronic Mail

6. Electronic communication such as e-mail that is strictly confined to intraorganization communication will not need boundary protection if disk boundary protection is enforced. External communications, other than those conducted via an air-gapped system, should only occur via one of the organization's servers. It is the Network Manager's responsibility to ensure that effective anti-virus software is installed which will check all incoming and outgoing mail for viruses before forwarding to its destination.

E-mail Scanner

7. This resides on a (firewall) server and scans all e-mail before it is passed through to the destination e-mail server. It is good network design to use this (on a server) in combination with on-access scanners on workstations.

Boundary Protection - Internet

8. Internet connections are only allowable with authorization from the appropriate accreditor. It is recommended that an air-gap be maintained between the Internet terminal and user systems. Files originating from the Internet should be transferred using a disk via the disk boundary facility.

Protection at User's Workstation

9. Boundary protection is very effective but it is still possible for viruses to reach the user's workstation via a number of loopholes. Unknown viruses will not be detected by

a signature scanner and may fool an heuristic scanner, but the biggest loophole is introduced by the increasingly common use of compression and encryption. It is not possible for any anti-virus product to expand or decrypt all files as many compression standards are used and 'blanket' decryption is not only virtually impossible but very undesirable. The best way of dealing with this is to install 'On access' scanners and/or activity monitors on the users' workstations.

Procedures to be used to Protect against Virus Attack

10. Procedures used to protect from virus attack must conform to the basic principles described below.

a. Users must be educated about the dangers of viruses including how to minimize the threat and how to recognize an attack.

b. All non-online input media must be checked for viruses on specifically allocated "sheep dip" PC(s) before they are permitted to be used on any user system. This includes software installation disks.

c. Anti-virus software listed in Defence Information Assurance Notice No5 should be used.

d. Anti-virus signature scanning software must be updated at least every month.

e. Only software authorized by ITSO shall be installed on any system. Checksumming of program files should be carried out to enable effective, regular auditing of user systems.

f. Direct connection to any external system shall only be made with the explicit permission of the appropriate accreditor(s).

g. Connection the Internet is forbidden unless specifically authorized by the ITSO and the appropriate accreditor(s).

h. On-line data sources must be controlled by a network/system manager to ensure that all incoming and outgoing data are checked for viruses.

i. The network manager of any system with external links must provide virus guard software to examine all incoming and outgoing mail.

j. At least one person in each organization must be identified as the local point of contact for advice and assistance on virus protection and incidents.

11. The additional measures below should be considered when feasible and appropriate.

a. Disk authorization packages can be used to prevent users using disks that have not been virus checked. This will also prevent the use of 'pirated' software.

b. Activity monitors installed on users' workstations will provide additional protection. A balance between protection and system performance needs to be reached, however, the performance degradation on modern workstations is now low.

c. On access scanners should be installed on users' workstations when a significant amount of compressed and/or encrypted data are used.

d. Regular auditing and scanning of user workstation files should be carried out. Ten percent spot-checking of user systems will act as a deterrent against the illicit installation of software and can be effective in detecting dormant viruses.

SECURITY OF PORTABLE CIS

This page intentionally left blank.

CHAPTER 8

SECURITY OF PORTABLE COMMUNICATIONS AND INFORMATION SYSTEMS

Introduction

0801. This Chapter gives guidance on the security requirements specific to portable Communications and Information Systems (CIS) in use within Defence.

0802. For the purposes of this document portable IT systems are defined as those systems for which it is envisaged that there will be no permanent local security environment. This introduces additional risks, particularly of theft and TEMPEST considerations. Such systems, with the appropriate security accreditation, can be used to produce data at any level of protective marking. Within the MOD, portable IT Systems are categorised as follows:

a. **Laptops.** Laptops, which include most notebooks and some palmtops, are Portable IT System equipped with the range of ports normally present on a standard PC.

b. **Personal Digital Assistants (PDA)** PDAs, sometimes referred to as Electronic Personal Organisers, include any such devices which are capable of storing magnetic data and exchanging such data with a PC but not equipped with the normal range of PC ports.

c. **Electronic Personal Diaries.** Electronic Personal Diaries are devices capable of storing data in a magnetic form but which cannot communicate with a PC.

0803. Portables do not include mobile systems such as those mounted on mobile military platforms which are covered in **Chapter 9, Deployable Systems**.

Background

0804. Portable CIS are valuable and powerful management tools which enable more flexible use of computing power. The inherent portability and power of such systems creates a significant degree of risk to security.

0805. In the past, the lack of any certified technical means to safeguard such systems led to the imposition of procedural safeguards which limited the use and effectiveness of this technology within the MOD. The MOD has been severely embarrassed in the past, not primarily by the loss of such devices, but by the potential compromise of data contained within them.

0806. To prevent future embarrassment, a trusted means of protection which will nullify the effects of a physical loss of such equipment can be employed. Evaluated and certified products which encrypt systems in their entirety are now becoming available enabling progressive liberalisation of the usage of Portable CIS. The policy on encryption set out in paras 0821 to 0828 below is specifically aimed at reducing the damage resulting from the loss or capture of Portable CIS.

Specific Regulations

0807. Accreditation All Portable CIS used to process official information must be registered in accordance with the regulations laid down in **Chapter 2**, which will include a "Authority for Carriage" letter. This includes, where applicable, the serial number of the cryptographic key in the list of software.

0808. The accreditation of Portable CIS recognises an authorized Home Base. When Portable CIS are removed from this Home Base they are to be accompanied by written authority showing details of the system, associated magnetic media and peripherals and their associated protective marking. **Annex A** gives a generic example of the letter of "Authority for Carriage".

0809. Privately owned Portable CIS are to be used in accordance with the regulations stipulated at **Chapter 1, Paragraphs 01091 - 01093**.

0810. Security Policy Documentation SyOPs must contain a synopsis of the conditions under which the equipment may or may not be used, including TEMPEST requirements. The SyOPs are to be carried with the system. An example of generic SyOPs for portable systems is at **Annex B**.

0811. Physical Security and Siting Portable CIS can normally be used in any official location in Great Britain, subject to any overriding local regulations with regard to their carriage into sensitive areas.

0812. Care must always be taken to ensure that protectively marked information cannot be overlooked by unauthorised persons.

0813. All magnetic disks, and other forms of memory storage which retain information when the power supply is disconnected are subject to the appropriate document security rules.

0814. Before importing portable equipment into any site, local security approval must

be obtained in advance, through the normal channels. The local rules in force for such documentation, such as gate passes, remain in force. The rules governing Homeworking are laid down in **Chapter 1 Annex E**.

0815. Installation Control All Portable CIS must meet MOD recognised EMC standards. Any system which is intended to process information protectively marked CONFIDENTIAL or above must have a TEMPEST certificate from an MOD TEMPEST authority, and may only be used in MOD or OGD controlled spaces which is already approved for processing of material at this level.

0816. In all cases the basic TEMPEST requirements for separation of protectively marked systems, whether the laptop or fixed installations nearby, must be adhered to, and care must be taken to site the Portable CIS away from telecommunications devices.

0817. Compliance ITSOs/BSOs must be provided with details of all portable CIS in their area of responsibility for which they will issue appropriate authority for carriage letters as laid down at **Annex A**. ITSOs/BSOs will be required to set up procedures to carry out random checks of any Portable CIS introduced into their area to ensure that the terms of their SPD are being met.

0818. Introduction of a privately owned Portable CIS onto MOD premises will be on the understanding that the ITSO/BSO, or other security staff, have the right to check that the use is within the regulations. At the discretion of, and if required by, the ITSO/BSO this may include providing full access to any private data.

0819. MOD security guards are advised to random check containers that could be used to carry portable CIS (i.e. bags) for the presence of such CIS, and, where found, may require the bearer to produce the form of authorisation for carriage as laid down at **Annex A**. Failure to produce such an authorisation may result in the temporary confiscation of the equipment until the responsible ITSO/BSO can be contacted.

0820. Interconnection Portable CIS must not be linked to any other CIS or network without prior security approval, including a Risk Assessment to the recipient CIS. Links via a PSTN modem, ISDN Terminal Adapter (TA), or other such device (e.g. embedded GSM in PDAs) across a public telephone system are forbidden, even for UNCLASSIFIED working, without the specific approval of the Accreditor.

0821. Portable CIS holding material protectively marked CONFIDENTIAL and above shall not be linked to the Internet.

0822. Encryption File based encryption products such as those incorporating Baseline Grade (BG) CESG approved algorithms (e.g. THAMES BRIDGE and RED PIKE) can safeguard material protectively marked up to RESTRICTED. Additionally, products such as KILGETTY and KILGETTY PLUS which provide full disk encryption, can provide protection up to and including CONFIDENTIAL and TOP

SECRET respectively. Further COTS products are being certified under the ITSEC scheme. Users seeking further advice on these devices should, in the first instance, contact the appropriate PSyA. The procedures for the procurement, distribution, accounting and use of Kilgetty within the MOD are described at **Annex A to Chapter 23**.

0823. The fitting and use of disk and file encryption products on officially provided Portable CIS is to be in accordance with the endorsed SPD. [Note: Disk and file encryption products are generally not available for Palmtops, Electronic Personal Organisers and some Notebooks.] They may process information up to the level of protection specified by the CESG algorithm provided with the product. Where approved encryption products are not mandated and cannot be employed, or are not considered necessary, then provided appropriate physical security measures are in place, it is still acceptable for protectively marked information to be processed on portable devices.

0824. The following rules apply to laptops taken outside the Global Security Environment, i.e. away from the authorized home base, or are liable to loss or capture.

a. Systems holding material protectively marked CONFIDENTIAL and above must have an evaluated full disk encryption product incorporating a CESG algorithm installed;

b. Systems with a full disk encryption product installed shall be protected at a minimum as RESTRICTED items when powered off;

c. Systems holding material protectively marked RESTRICTED and below must have an access control product from the MOD ICS catalogue installed.

0825. If there are any technical difficulties in applying this policy, advice is to be sought from the PSyA who can, exceptionally, exempt the requirement.

0826. The above policy represents the baseline standard. However the use of full disk encryption is recommended for all Portable CIS processing official information that are liable to removed from the Global Security Environment.

0827. Where a fixed hard drive is fitted to a system used to process and store protectively marked information and the encryption option has been chosen, in accordance with the regulations laid down in **Chapter 23,** the device must be installed before it leaves the users home base.

0828. If the disk encryption product incorporates a Touch Memory Device, the Token Key should be kept separate from the laptop whenever the Portable CIS is not in use or in transit, and removed from the laptop when left unattended.

0829. Disk encryption products are vulnerable when the system is connected to a public network. If a Portable CIS with a disk encryption product installed is to be connected to a public network an inline COMSEC device must also be installed. If a Portable CIS with disk encryption is lost or captured, and subsequently returned, the BIOS must be reset and the disk encryption product must be unloaded and a new version installed.

There are restrictions on the use and movement of cryptographic equipment abroad. If it is intended to take a Portable CIS employing encryption outside of Great Britain, advice should be sought from the PSyA via the security chain of command. Guidance on the export and import of KILGETTY and similar encryption devices is at **Annex B to Chapter 23**.

Transport of Portable Computers

0830. The normal rules for the carriage of protectively marked documents apply in all cases for the carriage of Portable CIS. Although encryption will permit the secure removal of protectively marked information from units or establishments, the procedures for this activity will largely relate to those already in place for hard copy protectively marked documents. Personnel will not be able to remove encrypted, protectively marked data without authority. The existing security regulations contained within JSP 440, Volume 1 must be adhered to.

0831. No Portable CIS may be used to process Protectively Marked information in a public place, or be taken abroad without the specific approval of the Accreditor.

0832. Portable CIS, in addition to the attractiveness of any Protectively Marked data contained, also constitute Valuable and Attractive (V&A) items, and if transported outside of MOD controlled areas are at significant risk of being stolen, both whilst in transport and if left unattended. The standard protective security regulations as laid down in Volume 1 for the protection of assets must therefore be followed.

0833. All new Portable CIS, other than handhelds, which are intended to be transported and/or used outside MOD controlled areas should be carried in a container whose external appearance does not draw attention to the probable, valuable and attractive, (V&A) nature of its contents (e.g for bags, neither being of a distinctive “laptop bag” design nor visibly bearing any computer manufacturers or suppliers label or logo). Any Legacy equipments should also be furnished with such a container if their residual lifetime exceeds 1 year. The required style of container is available from the MOD ICS catalogue.

Customs Issues

0834. When carrying any portable computers overseas, it is recommended that copies of software license agreements should be carried, as some Country's Customs Official may require proof that no new or illicit software is being transported.

0835. Additionally, it should be noted that Her Majesty's Customs and Excise (HMC&E) has introduced a policy of randomly carrying out technical scans of laptop computers for illicit material. **Chapter 11** provides some background on what may be regarded as illicit material, which is normally assumed to be the type of material of Indecent or Obscene nature banned from MOD systems.

0835 However, should a bearer of an official laptop be stopped by HMC&E who claim to require to scan this laptop, then the bearer is to direct that the matter must be referred to an appropriately cleared Investigation Officer, who should be contacted through:

HMC&E National Investigation Service
Custom House
Lower Thames Street
London EC3R 6EE
020-7283-5353 / 020-7665-8112 (FAX)

0836 The standard format of carriage approval at Annex A includes this information, and should be produced to HMC&E on request.

Handheld CIS Systems

0837 Officially provided Handheld CIS systems (including Palmtops, Personal Digital Assistants (PDA), and Electronic Personal Organisers), may be used to store and process information protectively marked up to and including RESTRICTED, provided that:

a. A password system of at least 8 characters is provided, which has been endorsed by MOD as having proved to be invoked under all circumstances. A current list of such approved PDAs is included in a Defence Information Assurance Notice (DIAN), and advice as to other such device can be obtained from EC-CCII-IOCM ;

b. The password has been generated using a CESG approved algorithm;

c. It is possible to disable all remote access facilities (e.g. IRDA and serial ports) when not required;

d. All removable media attached to the PDA must be afforded physical protection when unattended, as the password system would be unable to protect this if it were removed ;

e. SyOPs are provided for the system, to be signed by the user on a master copy before issue and also installed in soft copy on the system, including all the relevant requirements from **Chapter 3**, and the specific requirements from this chapter.

0838 Electronic Personal Diaries are not to be used for the storage of protectively marked data.

0838 Handheld CIS must not be linked to any other CIS or network without prior security approval, including a Risk Assessment to the recipient CIS. Data may be exchanged with a standalone PC provided the exchange is permitted by the SPD for the PC and the SPD for the organiser. The PC must have current 'On-access' anti-virus software (AVS), installed which is updated regularly, as laid down at **Chapter 7.** Such exchanges of data are to be limited to PCs operating at RESTRICTED and below.

This page intentionally left blank.

ANNEX A TO CHAPTER 8

GENERIC AUTHORITY FOR CARRIAGE LETTER FOR PORTABLE IT SYSTEMS

On Official Letterhead :

FOR ATTENTION OF :

All HQ and Service Gate / Door Guards
[Customs Authorities and Border Police]

AUTHORISATION FOR CARRIAGE OF PERSONAL COMPUTER EQUIPMENTS

References:
A. JSP440 (Defence Manual of Security) Volume 3 (CIS)
B. Wassenaar Agreement
C. NATO Status of Visiting Forces Agreements
D. US International Traffic in Arms Regulations (ITAR)

Identification

1. In accordance with Reference A, it is hereby certified that the following officer ("The Bearer") is authorised to carry and use Official portable computer equipments :

Rank/ Title	
Name	
Post	
Service/Staff Number	
ID Card Number	

Authorised Equipments

2. This authorisation applies to the following equipments, which are declared to be property of Her Majesty's Government :

Unit Type	Make	Model	Serial Number
Portable Computer			
Removable Hard Disc			
Portable Printer			

Security Approval

3. This authorisation permits the use of the equipments at up to a <Protective Marking> level of Protective Marking, in accordance with the Registration Document/System Policy Documentation (SPD) and Security Operating Procedures (SyOPs) which are to be carried with the equipment.

Import and Export to European Union (EU) Countries

4. In accordance with References A and B, it is declared that any encryption technology used within these equipments are not capable of online voice encryption or decryption, are designed to be used in conjunction with digital computers, and are intended for the personal use of the Bearer. Export Licence Exemption is therefore claimed.

Import and Export to United States of America (USA)

5. In accordance with References C and D, it is declared that the Bearer is a British Government Official on Temporary Duty (TDY) within North America, as confirmed by <US "A2" Visa *nnnnn* in British Passport Number *nnnnn* > / <NATO Travel Order F/Mov/220 Serial Number *nnnnn*>, and that any encryption technology used within these equipments is solely intended for personal and Official use. ITAR Exemption is therefore claimed.

6. Any queries relating to the Bearer whilst in the USA should be addressed to:

Defence Staff Duty Officer
British Embassy, 3100 Massachusetts Avenue NW
Washington DC20008-3600
(202)588-6868 / (202)588-7888 (FAX)

Return of Equipment to UK

7. It has been agreed with Her Majesty's Customs and Excise (HMC&E) that should a Customs Officer at port of entry declare a requirement to scan the media associated with these Portable Computer Equipments, the Bearer is to direct that the matter must be referred to an appropriately cleared Investigation Officer, who should be contacted through:

HMC&E National Investigation Service
Custom House
Lower Thames Street
London EC3R 6EE
0207-283-5353 / 0207-665-8112 (FAX)

8. Should you require any further information, please contact the undersigned.

<*Signature*>
<Name>
<Rank/Grade>
<Establishment>/<Branch> Security Officer

NOTES FOR COMPLETION

a. Delete paragraphs not required, e.g. for a portable computer that is only to be used in UK delete references B, C and D and paragraphs 4, 5, 6 and 7.

b. Refer to Annex B of chapter 23 for countries to be visited other than EU or USA and create new paragraph similar to current paragraph 4.

This page intentionally left blank.

ANNEX B TO CHAPTER 8

GENERIC SyOPs FOR PORTABLE IT SYSTEMS

Introduction

1. This document constitutes the System Policy Documentation (SPD) and the Security Operating Procedures (SyOPs) for the IT portable computer system as detailed in the attached registration form. They are issued by the ITSO in accordance with the Defence Manual of Security, and have been approved by the Accreditor. All personnel using the systems are to comply with these SyOPs, and no departure from or amendment to them is permitted unless prior authorization is obtained from Accreditor.

2. Breaches of these orders may render the offender liable to disciplinary action.

Administration

3. The ITSO for this system is:

Job Title:
Branch:
Tel No:

4. The ESyO for this system is:

Job Title:
Branch:
Tel No:

5. Where applicable, authorized users of this system are listed at ANNEX A. Additions to the list of authorized users must be approved by the ITSO. Where there is only one authorized user Annex A need not be completed and users details should be entered here.

6. The highest protective marking of material which may be held or processed on this system is: ..... Systems are only approved for the processing sessions and protective markings of material as specified in the registration form.

Personnel Security

7. All authorized users of this system must have the appropriate security clearance for the material processed on the system. (Basic Check (BC), Security Vetted (SV) etc). If need to know separation is necessary, users should not share magnetic media, unless

trusted partitioning is available.

Physical Security

8. The system is normally based in ..... and must not be removed without the permission of the ESyO or ITSO. In addition a register must be maintained showing the occurrences of removal of the system from its location. This register should show the date of removal, responsible officer, location system taken to, and the date the equipment was returned.

9. When not in use the system and any associated magnetic media, eg. floppy discs, removable hard discs, etc, must be protected and handled in a manner commensurate with the highest protective marking of material processed on the system.

10. Outside secure Defence environments the equipment may only be used for unclassified work (ie. below RESTRICTED) unless specific permission for protectively marked work has been given by the appropriate security authority. While equipment and associated removable media are in transit outside a secure MOD environment, the media should be carried separately from the equipment.

11. The equipment must not be operated within # metres of telephones, other communication devices or any other electrical equipment processing protectively marked information. (# metres to be defined for the system) No connection is to be made to any Fax/Modem or other such device without the approval of the security authority.

Document Security

12. The term 'documentation' in this context refers to any information-bearing part of the system and includes floppy discs, removable hard discs, magnetic tape, internal non-volatile storage and printer ribbons.

13. All magnetic media is to be uniquely marked and registered in accordance with Security Regulations. Unless declassified by data destruction (see Annex C to Chapter 4) the protective markings of magnetic media will be retained and will determine the eventual method of disposal of the media.

14. Document and equipment disposal must conform with the regulations pertaining to the highest protective marking of material held on or processed by the system.

15. Information displayed on the VDU screen must be protected from overlooking by unauthorized persons.

Hardware Security

16. Equipment must be checked before use for obvious signs of tampering. Any

suspected problems should be reported to the ITSO without delay and the equipment should not be used until checked and cleared.

17. Staff must declare the equipment in advance when visiting other organizations and be prepared to forego its use in sensitive areas.

18. All protectively marked material is, where possible, to be removed from the equipment before maintenance engineers are allowed access to it. Unless appropriately security cleared engineers must be supervised whilst they are working on the equipment.

19. All magnetic media introduced to the system by an engineer for diagnostic purposes must be checked for viruses first. All magnetic media used on the system and faulty items removed from the systems must be treated in accordance with the security measures appropriate to the highest protective marking of data held on the system; this will normally result in such items being retained on Defence systems.

20. No item of equipment which may contain protectively marked material may be removed from MOD premises for repair without permission from the appropriate security authority. Where such permission cannot be given repair of the equipment will be by total replacement of the faulty part(s) and the damaged component(s) must be retained and destroyed in a manner commensurate with the potential protective marking. Where protectively marked data is involved any magnetic media used by an engineer for diagnostic purposes must be retained and the security measures pertaining to other magnetic media apply.

21. All hardware failures must be reported to the SM who will arrange for the necessary maintenance and maintain the records of system failures.

Software Security

22. All software used on the system is to be from authorized sources and properly licensed. Software may only be installed with the express authority of the ITSO and after the installation disks have been checked for viruses.

23. Back-up copies should be made of any software or data essential to the operation of the system. These should be kept in a different location to the working copies of the software and data files. Back-up copies should be made frequently and an annual test should be conducted to verify that the back-up copies are usable.

24. Any suspected attack by a virus or other subversive software must be reported to the ITSO without delay and the system should not be used until a security investigation has been carried out. #Insert after here either the full rules from DMS Vol 3 of the actions to be taken or refer to the chapters and paragraphs. This will depend on whether the machine is to used solely on Defence sites.#

Accounting And Audit

25. Information held on portable computer equipment and associated magnetic media is subject to the same degree of audit as that held in other forms eg. paper.

Losses And Breaches

26. Any incident involving a breach of personnel, hardware, software, document, or physical security is to be reported immediately to the ITSO.

Backup Procedures

27. Individual users are responsible for ensuring that back-up copies of any data files essential to their work are adequately maintained.

Virus Protection

28. 'On-access' virus protection software must be installed and active at all times. The installed anti-virus software must be updated on a regular (monthly or better) basis. If the home base employs 'boundary virus protection', all disks used on the portable system must be treated in the same way as a system in an external organization.

29. The following procedures should be followed to provide additional protection:

a. All exchange media are to be write protected once prepared.

b. Unless explicit permission is given by the system manager, only data files may be copied.

c. As soon as the copy has been carried out, the transfer diskette must be returned to the originator. Under NO circumstance is the system to be rebooted while the exchange media is in place.

d. The system manager should change the BIOS settings to force system to look for the boot-up sector on the C: drive before looking at the A: drive.

30. If a virus attack is suspected the following actions must be taken.

a. STOP USING THE WORKSTATION AT ONCE.

b. The system is quarantined, along with all media associated with it.

c. Do not switch off or re-boot the system until being given permission to do so by local or PSyA.

d. Inform the system manager and ITSO immediately.

e. Locate and isolate all disks and other i/o media which may have been used on the infected workstation.

f. Identify and isolate any workstation which may have been infected.

g. Identify and warn any users that may have been sent infected files.

31. Recovery of data must not be started until the ITSO is satisfied that any investigation will not be compromised and gives explicit permission to begin. Virus scanning and eradication of viruses from suspect workstations and disks is only to be carried out by personnel specifically authorized to do so by PSyA.

32. Where the anti-virus strategy incorporates the use of a central "sheep dip" facility, reinforced by the use of a workstation media authorization guard (WMAG), the WMAG package must be set for a specific protective marking level. If there are systems working at different protective marking levels, the WMAG must be set on a separate machine for each protective marking level. End user systems should not contain software capable of subverting the WMAG mechanism such as primitive level disk editors.

This page intentionally left blank.

DEPLOYABLE CIS
(CIS SECURITY ON OPERATIONS)

This page intentionally left blank

CHAPTER 9

DEPLOYABLE CIS
(CIS SECURITY ON OPERATIONS)

General

0901. Most CIS are in static environments with established physical security and known threats. CIS security on operations must be appropriate for a range of threats and changes of physical environments. Deployments are now commonly made by multi-national ad hoc HQs, frequently with commercial equipment. Hence, the enforcement of CIS security countermeasures on operations requires personnel with the appropriate engineering skills, authority, responsibility and training

0902. **Volume 1 Chapter 14** sets out the requirements for Security on Operations. **Sub-para 1414.d.** requires that appropriate protective measures for IT systems on such deployments are to be set out in System Policy Documentation (SPD) and Security Operating Procedures (SyOPs) but gives no explicit advice. **Volume 1 Chapter 14 Annexes C and D** give advice on the protection of documents and equipment but make no specific reference to IT systems, although it should be noted that electronic media, such as disks, are to be treated as documents. With the advent of an increasing number of actual and planned IT infrastructures for use in field situations it is now necessary to promulgate a consistent policy for all systems based on existing custom and practice. This chapter applies to CIS Security on exercises or operations on land.

Phases of a Deployment

0903. A typical deployment may comprise one or all of the following phases for which the threats and appropriate actions will differ:

a. **Pre-Deployment Phase**: identifying equipment types, vehicle fits, security awareness training (which should be repeated throughout a deployment) IT policies, confirmation for regularly updating anti-virus software in theatre and accreditation.

b. **Short duration locations phase**: countermeasures for a mainly spatial RF threat and a limited line conduction threat. During a mobile phase, installation security is achieved by filtering vehicles correctly and interlinking them in an approved manner. This phase will not normally exceed 7 days at an individual location.

c. **Medium duration locations phase**: countermeasures for a controlled migration plan, from management of limited threats, to management of all static installation threats. This plan will include liaison with communications and information systems project managers, Design Authorities, RADSEC Inspections Units and Security Inspection Units and PSyA.

Responsibilities

0904. The commander at every level is responsible for security within that command. Security should enhance an operation; not constrain it. Nevertheless, the compromise of security could well have much wider consequences than within the command itself or the particular operation and this must be taken into account by commanders when managing the risks involved. Commanders are to ensure that all IT assets within their command have current accreditation.

0905. Operational deployments may be UK national, NATO or some form of international coalition. Security of UK national information remains a national responsibility and a Commander British Forces (COMBRITFOR) and a UK Chief of Security Staff are normally appointed with staff control of UK national Field Security Detachment(s) (FSDs). The national information Security Authority will often be separate from the Joint Service or International higher command Headquarters (HQ). Authority to release information, even to allies, must be confirmed not assumed.

0906. System accreditation covers the electronic environment inside each system and the local environment that is controlled by the users of the system. The global environment (controlled site) surrounding this local environment is controlled by or on behalf of the joint or international higher HQ as part of the general security requirement following the general security policy of that HQ. Authority to accredit some minor CIS may be delegated to staff or units in theatre.

0907. The responsibilities of a System Operating Authority, as detailed at **Annex B to Chapter 2,** may be split between a central (normally UK based) continuity post enacting whole life system management (configuration control board chair, authorising system enhancements, disposal, etc) and a deployed (possibly roulement) local system management post enforcing system security.

0908. Physical security measures for IT systems are described in **Chapter 5**. The commander of a site is responsible for ensuring that systems within the site are properly accredited and installed and that security procedures are followed. He may delegate authority for these security enforcing functions to an IT Security Officer (ITSO) as detailed at **Annex A to Chapter 2** and to a RADSEC Control Officer (RCO) as detailed at **Annex E to Chapter 21**. Additional CIS equipment brought into a site is to be "adopted" both by the RCO for installation practice and by the ITSO for confirmation that user security procedures are held and followed. Deployment RCO and ITSO are required to provide security advice in roles where they may be isolated

from support for extended periods of time. The RCO must therefore be experienced in both general installations and TEMPEST matters and the ITSO must be experienced in both general and procedural security.

0909. The enforcement of security installation standards needs to have a focus of accountability for the whole site. The RCO must work closely with the CIDA and RADSEC Inspection Unit. The RCO should normally be the engineering officer responsible for the largest installation on the site. The critical factor is that the individual needs to be clearly nominated and given sufficient authority.

0910. Every individual who handles protectively marked or vital information and material is personally responsible for safeguarding it in the appropriate manner. Normally, only individuals who have been explicitly approved are to have access to such information and material. SyOPs are to address this issue in detail. To assist availability, security documentation should preferably be on the system or in soft copy.

Additional Vulnerabilities

0911. Some of the additional vulnerabilities arising from operational deployments are as follows:

a. Fluid operations with frequent changes of locations and affiliations may prevent the establishment of normal procedures and demand constant improvisation. There is a consequent temptation to meet short-term goals at the cost of longer-term dangers.

b. Guard forces are likely to be very few and combine a number of functions.

c. Individuals are more likely to make mistakes and neglect duties due to extreme physical conditions and tiredness.

Use Of Unprotected Media

0912. Regulations for the control of private correspondence and telephone calls are described in **Volume 1 Chapter 14 Annex E**. These principles apply to the use of unprotected means whether private or officially provided as follows:

a. Conversations in unprotected areas must avoid official protectively marked information.

b. Discussions/briefing must only take place in areas where counter-eavesdropping has been considered and appropriately implemented.

c. Private correspondence and telephone calls - as above.

d. Protectively marked information in official correspondence and telephone calls must be within the protective marking appropriate to the means being used.

e. Private or official Internet use must avoid official protectively marked information.

f. Private or official commercial CIS use, e.g. flight bookings, must only include the minimum essential official information.

Threat Assessment

0913. A statement of generic threat to IT systems is given at **Annex B to Chapter 3**. This can be customised for IT systems intended for deployment within the SSP. When a system is deployed to a new theatre of operations, the accreditor is to be notified so that the predicted threat may be validated against the current threat, and appropriate additional countermeasures, relaxations or waivers adopted. If the system manager is notified of a change of threat, this is to be passed to the accreditor.

0914. IT systems are a principal source of information from which the enemy and other potential attackers will attempt to derive information. Additional threats, to those given at **Annex B to Chapter 3**, are as follows:

a. The primary risk to CIS on operations is loss of data either by capture or physical loss/damage.

b. Enemy intelligence services, and possibly co-belligerents, can be expected to task human intelligence sources at deployed systems. This is particularly likely where the surrounding civil population can be subverted by the interested party.

c. Operations, and some training, can expect to attract media attention. The publication of consequent reports may well have negative effects on operations.

d. The level and type of threat will vary over time and must be kept under constant review. Thus in static operations, espionage may be a major threat whereas in mobile operations the risk of loss and capture is more significant. IT systems which are intended for deployment on operations are to have appropriate countermeasures detailed in their SSP and SyOPs.

0915. IT systems intended for deployment are accredited against a generic set of threat, information types, user types, location types, interconnection requirements and management control with agreed countermeasures. Whilst many systems are used as predicted, operational circumstances can change the system requirements and available

resources. Unsanctioned changes may cause an unnecessary risk and invalidate the authority to operate the system. The proposed change must be detailed to the accreditor and a waiver sought. For installations, the RCO may authorise changes on behalf of the CIDA but must notify both CIDA and the accreditor if national minimum standards cannot be met and seek a waiver.

Countermeasures

0916. **Collective Security (The Global Environment)**. IT systems do not exist in a vacuum. They can expect to receive considerable protection from the surrounding environment in which they are located. This will range from the conceptual, such as policy on personnel vetting or the release of information, to the severely practical, such as the provision of guards. The following are particular measures to be included in SyOPs.

a. Wherever practicable, IT system hardware should be located within a location offering a degree of collective security. Where CONFIDENTIAL, or higher, information is being processed it will be normal to establish a defined and guarded perimeter, with controlled access of all entrants. This is primarily designed to exclude unauthorised non-belligerents, such as the local population and the media.

b. Plans are to be made for the destruction of all information or material if capture appears likely. Particular attention is to be given to establishing who can give such instructions and the priority and methodology of carrying out the orders.

c. The grouping of IT systems, and particularly radios, in a close environment can cause problems with the unintentional radiation of protectively marked information. It is particularly important that TEMPEST precautions are followed and that, in larger HQs, a TEMPEST control officer is designated.

0917. **Local Security**. Within a field environment, significant responsibility is placed on individuals (or groups of individuals) to protect equipment, such as weapons, placed in their care. IT equipment follows the same principles and the following measures are to be addressed in SyOPs:

a. The issue and receipt of all IT equipment or documents to the care of individuals or groups is to be recorded. Where this is SECRET or higher this is to be entered in a Protectively Marked Documents Register.

b. Equipment and documents are to be physically checked before and after all moves.

c. Only essential equipment and documentation is to be held in the field. All protectively marked assets no longer required are to be backloaded or archived, deleted or destroyed. Even though simple electronic deletion of IT records provides no defence against a determined analysis, it does offer considerable protection from rapid assessment.

d. Access to IT equipment or media handling CONFIDENTIAL or above information is to be strictly controlled. Normally access control by a Simplex lock into a selected room will be sufficient to prevent access by unauthorised personnel. Unattended vehicles are to be protected by a security padlock and protectively marked material removed if possible. Such measures are reinforced by password mechanisms and screen-saver protection when an IT terminal is not manned.

0918. **Electronic Security**. Within IT systems it is usual for the system itself to enforce security, using software, cryptography and so on. From the user point of view this is initiated by the entry of a password on the system, which allows it to identify a role and permit access to certain resources. In static situations it will be normal to allocate passwords to individuals to enforce accountability at this level. At the discretion of local System Manager it is permissible to amend this rule as follows:

a. Should the operational situation require it, a single role and password may be shared by a number of staff users only if a paper record is maintained as to who had access to a work station at any time (by use of a shift log etc.) The local system manager is to record the decision to use group passwords and the situation that justified their use. Such paper records are to be retained for a period of 5 years.

b. This approach is not to be followed for privileged users, such as system administrators, who are to retain their individual identity on the system.

c. As soon as practicable, the use of group passwords is to be discontinued.

0919. At some sites, WMAG communities between systems may be appropriate with a standalone "sheep dip" PC to allow virus checking of floppy discs from outside sources to be separate from the system on which processing takes place. This enables identification and exclusion of new viruses that might not be eradicated by the current version of antivirus software, without contamination of the destination system.

0920. All new system interconnections or PSTN connections, especially to the Internet, can introduce additional vulnerabilities and these must be already covered by the SSP or specifically approved by the accreditor.

Maintenance And Disposal Of Equipment

0921. It is possible to modify electrical equipment to enhance its radiation or to change its electronic performance. Where equipment is deployed, it is to be given appropriate physical protection and periodic inspections to detect tampering. Maintenance is to be carried out by, or under the supervision of, technically qualified appropriately security cleared personnel. Supplementary or replacement equipment is not to be procured or hired in a deployed theatre unless authorised by the accreditor. Equipment and media that has held protectively marked information is to be destroyed or returned to UK for disposal in accordance with **Chapter 4**.

Emergency And Contingency Plans

0922. Recommendations for content of emergency and contingency plans are given in **Chapter 3**. These plans are particularly important to describe backups and alternatives where some services are outside MOD control. The granularity of the plans will vary between locations and duration of occupancy.

Compliance Activities

0923. Notification to the Security Authority of the deployment of a system on operations is a trigger for several compliance activities as follows:

a. Confirmation of reporting chains.

b. Confirmation of system audit activities.

c. Monitoring as appropriate.

d. Theatre or specialist inspections at frequencies appropriate to the system.

e. Facilities for investigations of reported incidents or security breaches.

Further Advice

0924. CIS Security on operations is a complex and developing field, advice is available and should be sought from theatre J2 staff, PSyA and Senior HQ security staff as required.

This page intentionally left blank

INTERNET SECURITY

This page intentionally left blank.

CHAPTER 10

INTERNET SECURITY

Introduction

1001. The Internet provides a means of connecting computers around the world. It is an open environment, whose whole purpose is to facilitate the exchange of information. However, its very openness also makes it vulnerable to security threats. The Internet is a public network that has no central management or control. The user has no control over the route a message will take when it crosses the Internet and it is possible for messages to be read or modified. Connection of a system to the Internet makes it vulnerable to other Internet users with malicious intent. Even though a very tiny minority of users will attempt to steal, alter or delete information or disrupt services and systems, the risk will always be there.

1002. The more common uses of the Internet include:

a. E-mail, which allows the exchange of mail messages with other users anywhere in the world. E-mail is more than a messaging service as it provides the facility to append a variety of attachments;

b. World Wide Web is a multi-media environment for publishing and sharing information on the Internet. It provides access to millions of documents, called Web pages. The documents can be in a variety of formats including plain text, files, pictures and video;

c. Information Exchange (file transfer) provides the facility to send and receive virtually any type of data file, software programme, text, graphics video and sound across the Internet. These will often be appended as attachments to e-mail messages;

d. E-Commerce and Electronic Data Interchange (EDI) by which companies, organisations and individuals conduct business over the Internet. Information is exchanged using a combination of structured messages (EDI), unstructured messages (e-mail), data, databases and database access.

1003. The security issues for each of the above services are included in the table at **Annex A**.

1004. Connection to public data networks such as Internet is becoming an essential requirement for many Defence applications. Such connections are inherently insecure and, although some security measures may help, there is currently no completely trusted method of protecting systems, which are connected to the Internet. Consequently it is

important to ensure that the appropriate security controls and procedures are implemented to protect MOD assets.

1005. Malicious software poses by far the greatest risk to Internet users. It is vital that adequate protective measures, as detailed at **Chapter 7**, are introduced to diminish the risk of virus infection spreading from an Internet connected system or terminal to other systems within an organisation.

1006. Hacking, unauthorised release and interception are the other significant risks associated with connection to the Internet.

1007. Users of any MOD system considering connection to the Internet must understand the risks of taking such action and ensure that the security policy detailed below, which also applies to other public data networks, is followed in all cases.

Authority To Connect

1008. Authority to connect to the Internet from within the MOD is retained at TLB or Trading Fund level. Applications are to be made through the local IT Security Officer (ITSO), Branch Security Officer (BSO) or equivalent to the appropriate Principal Security Advisor (PSyA) and the Coordinating Installation Design Authority (CIDA).

1009. Due to the very public nature of the Internet, security relevant incidents which relate to its use by MOD are likely to attract a much greater amount of unfavourable reaction from both the Press and, potentially, Parliament, than the perceived impact of the incident in simple (Confidentially) terms would suggest. Security staffs therefore may require in the event of such incidents to direct that connection to the Internet be severed until appropriate remediation can be applied.

Requirements For Connection

1010. Direct connection to, or to any system onwardly connected to, the Internet may be permitted under controlled conditions.

1011. All systems must have appropriate Security Policy Documentation (SPD) as laid down at **Chapter 3**. For standalone systems this will typically be a set of Security Operating Procedures (SyOPs) expanded to include basic configuration details, which are to be approved by the appropriate PSyA. All systems connected to, or to any system onwardly connected to, the Internet must be accredited. Only authorised personnel should be permitted to use the system.

1012. The system to be connected should normally be dedicated to the role and process only non-protectively marked (i.e. UNCLASSIFIED) information. Protectively marked material must not be published on the Internet. Any official information processed, which is not for public view should be segregated by use of a firewall or

similar product, the sophistication of which will depend on the quantity and type of information held on the system.

1013. The provision of telephone or other communications lines, which may be used to provide Internet, access will vary depending on local circumstances. In all cases, however, potential users must seek the advice of both the appropriate PSyA and the Authorised Telecommunications Officer (ATO).

1014. Connection to the Internet must be via a Secure Managed Connection as detailed at **Chapter 15**, other than in the case of standalone machines working in Dedicated Mode where the specific regulations laid down later in this Chapter will apply. The Defence Communications Services Agency (DCSA) provides the Internet Gateway Service (IGS) as part of the Restricted LAN Interconnect (RLI) initiative which is the preferred method of gaining connection to the Internet for those with RLI connectivity, and other internet connection routes for systems connected to the RLI will require their security arrangements to be coherent with this corporate approach.

1015. Gaining a connection to the Internet also requires prior approval from the sector Co-ordinating Installation Design Authority (CIDA). The CIDA is concerned with the load on telecommunications networks and the security of the proposed installation, including the risk of TEMPEST (the leakage of electromagnetic radiation from computer equipment which could potentially compromise secure data on nearby machines). As a result of this approval process, it may be necessary to make changes to the physical layout of the office. The CIDAs are listed in **Chapter 2 Annex E**.

1016. If it is required to connect a system which processes RESTRICTED information to the Internet, a firewall must be used to constrain access from the outside and to limit Internet services available to internal users, other than in the case of standalone machines working in Dedicated Mode where the specific regulations laid down later in this Chapter will apply. The firewall used to segregate and protect this information must be certified under either the Common Criteria or ITSEC schemes, typically to EAL4/E3 assurance level. Appropriate firewall properties and configuration advice are detailed in CESG Compusec Memorandum No. 13, as supplemented by the advice laid down at **Chapter 15**.

1017. The approval of the PSyA must be obtained prior to connection. In addition to clearly detailing the requirement and the protectively marked information involved, the case to connect must demonstrate fully that an assessment of the risks has been undertaken and any residual risk accepted.

1018. Any intention to connect a system processing information protectively marked at CONFIDENTIAL or SECRET to the Internet must be referred to InfoSy(Tech) within DDefSy for endorsement. The connection of systems used to store, process or forward information protectively marked above SECRET, or compartmented information, is prohibited.

1019. It is permissible for standalone systems to be used for non-Internet tasks provided a separate removable had disk is used and that this is not used when the system is connected to the Internet.

1020. Users of stand-alone Unclassified systems attached to the Internet should ensure that the information held or created, does not, by virtue of its nature or aggregation, warrant upgrade to a higher level of protective marking. If this does occur, the information should be removed to a different system and the hard disk used during connection to the Internet must be overwritten in accordance with the procedures in **Chapter 4**.

1021. Transfer of information from a system connected to the Internet must follow the policy and procedures set out in **Chapter 7** for checking for the presence of viruses and other malicious software. Extreme care must be taken if importing executable code.

Transmission Across The Internet

1022. The use of the Internet for transmission of material protectively marked CONFIDENTIAL and above is prohibited. RESTRICTED material transmitted across the Internet must be protected by a product approved by CESG as meeting Baseline Grade (BG) encryption standards. Such products can be obtained from the Software Security section of the DCSA Catalogue.

1023. National policy allows the use of encryption products incorporating Public Domain (PD) algorithms for Baseline encryption and applies primarily where there is a requirement to protect information for confidentiality. Baseline products will normally be developed commercially and evaluated by CESG for government use through the CESG Assisted Products Scheme (CAPS) prior to their inclusion on the DCSA Catalogue. Further information on the application of cryptography is at **para 1044** and **Chapter 23**.

Naming And Addressing-

1024. MOD, through DCSA, is registered with both Nominet and FIRST as the owner of an Internet "Class A" domain (*'.mod.uk'* and *'.mil.uk'*), and 2 Class B domains, *'dstl. gov.uk'* / *'dera.gov.uk' / 'dera.hmg.gb'* domain operated by DSTL, and *'moduk.org' / 'bdsw.org'* , operated by BDS(W).

1025. Beneath these High Level Domain (HLD), MOD units and formations can register sub-domains, and advice on acquiring Official domain names can be obtained from DCSA CM DNAA on Copenacre Military (01225-81-) 3379.

1026. FIRST is the international Federation of Incident Response and Security Teams, which, amongst other activities, takes responsibility for assigning focal points for Internet domains.

1027. The MOD Computer Emergency Response Team (MODCERT) is a distributed organisation within MOD registered with FIRST as being the competent authority for all Official domains, with the Joint Security Co-ordination Centre (JSyCC) in DDefSy functioning as its focal point.

1028. All MOD Internet facilities must use these Official domains, and Legacy domain names not complying with these conventions must be migrated to an Official domain name by February 2002. In certain cases other additional domain names may also be used, with the justifications normally accepted being :

a. Where there has been prior (Legacy) use of a non-Official domain for a publicly known Internet facility, such as a website or widely distributed email address, and where the immediate cessation of such a domain could cause a loss of communications. The need for such additional external domains should be reviewed on a regular basis ;

b. Where the unit or formation deals with the general public, and there are concerns that a domain name could accidentally or deliberately be generated that may appear to those not aware of the MOD's domain policy as an Official address. In such cases (e.g. MODCERT) registration of the relevant .ORG and .ORG.UK domains will normally suffice to "preserve the brand".

1029. In all cases where external domains are to be used, DCSA CM DNAA and DCCS(IN) must be informed, the primary website and email addresses must be set up on, or migrated to, an Official domain, and redirection emplaced on the external domain to the Official domain. It is permitted to retain a single redirection webpage on such external domains, which should contain the following information :

a. Name and Contact details of Unit or Formation ;

b. Short UNCLASSIFIED description of nature Unit and Formation, which should be cleared through the appropriate release authority ;

c. Details of, and Link to, Official domain.

1030. Exceptionally, where there is a need to preserve anonymity (although it should be stated that this does not represent any realistic form of security), users may wish to use a non-official email address, and in such cases specific approval must be sought from the PSyA or DSSO.

Software Security Issues

1031. The technological solutions to protecting networked or distributed system when connected to the Internet are beyond the scope of this Chapter. Specific advice must be sought from the system(s)'s Accreditor(s), with background information being provided

at **Chapter 15** (Security of Interconnected CIS), which covers the functionality of Secure Managed Interfaces (SMI), and **Chapter 24** (Use of Public Bearers).

1032. For simple, standalone, Unclassified systems being connected to the Internet however, the SMI can be constituted with the following software functionalities as a minimum which can be considered to provide some measure of Integrity and Availability protection:

a. Anti Virus Software (AVS), as detailed in more depth at **Chapter 7**;

b. IP port protection software to prevent, and preferably detect, unauthorised attempts to connect to TCP and UDP port services;

1033. Where standalone RESTRICTED systems are required to be connected to the Internet, the Accreditor, who must be either the PSyA or the DSSO, will also wish to satisfied that the system provides:

a. File system access control permissions, achieved either through the facilities built into the operating system (e.g. Windows NT Access Control Lists), or by an add-in software package. In order for this facility to work, different user logons will be required for access to RESTRICTED and UNCLASSIFIED (Internet) ;

b. Appropriate encryption software if RESTRICTED material is to be transmitted over the Internet. In order for this facility to work, a transfer folder will need to be configured that allows material to be moved between the RESTRICTED and UNCLASSIFIED user logons.

Incident Handling

1034. Any abnormal security related conditions identified by a user must be reported to the security authorities as well as to technical support staff. The normal incident reporting methods are to be applied. The rules for incident handling are covered in detail in **Chapter 11,** and it is stressed that due to the pervasive nature of the Internet, timely reporting of incidents is vital.

Compliance

1035. The controls that have been implemented should be regularly reviewed to ensure that they are being used properly and that they still provide the level of protection that meets the security requirement.

1036. All CIS that is used to store, process, or forward Official MOD information remains liable to Compliance Checking, as laid down at **Chapter 12**.

E-Mail Security

1037. Official e-mail addresses should, wherever possible, conform to the naming and addressing standard as specified by the Defence Message Handling Sub Committee (DMHSC) and should be disclosed with discretion and only used for official business. They are to use Official Internet Domain Names and their associated Mail Exchange (MX) e-mail addresses as laid down earlier in this Chapter.

1038. Unless the e-mail service is provided from a MOD infrastructure with a pre-assigned *'.mod.uk'* / *'.mil.uk', '.dstl.gov.uk', or '.moduk.org'* address, there are 2 ways to achieve a *'.mod.uk'* / *'.mil.uk'* e-mail address :

a. To use a Mail Redirector service whereby the outgoing message header, and incoming address, are aliased to a *'.mod.uk'* / *'.mil.uk'* address whilst actually using another "true" mailbox name;

b. For the Internet Service Provider (ISP) to attempt to obtain approval from DCSA CM DNAA to operate a *'.mod.uk'* / *'.mil.uk'* domain on behalf of the MOD.

1039. Although it is unlikely that mail hosts will afford users with the opportunity to automatically generate strong (CESG approved) passwords, where the user is given the option to choose the mailbox password then these should be selected in accordance with the guidelines given at **Chapter 6 Annex A**.

1040. There are potential dangers in using e-mail and that these particularly relate to the legal ability to access interpersonal e-mail and the capability of e-mail systems to retain messages deleted by the sender. In addition e-mail messages may be disseminated to, and therefore retained by, a much wider audience than the sender intended. Close attention should be paid to the protective marking of material and the factual content of e-mail messages.

1041. There may be occasions when it is deemed appropriate to use a disclaimer in an e-mail. Disclaimers should not be used routinely as the message is devalued and could be deemed to be meaningless legally or contractually. Three examples of instances in which disclaimers could be used are:

a. **Contract.** The e-mail is not intended nor should be taken to create any legal relations, contractual or otherwise;

b. **Private opinion.** The e-mail represents the personal views of the author/sender. The author/sender has no authority or delegation to bind the Department by the e-mail and the Department accepts no responsibility for its content;

c. **Confidence.** The e-mail is communicated in confidence. It is intended for the recipient only and may not be disclosed further without the express consent of the sender.

Mail Servers

1042. Any mail servers connected to the internet should be configured not to return "user not known" or similar responses, as the probing of mail servers by random email addresses for such responses is a well known technique used by attackers to carry out a reconnaisance of systems.

1043. All email servers connected to the internet must be configured to preclude their operation as Open Mail Relays. This is an essential attribute for all MOD email servers, aimed at prevent unauthorized users from utilizing MOD assets for purposes such as anonymous, abusive or bulk mailings, which can lead to offending servers being blacklisted and thus rendered unusable.

Cryptography

1044. Material not attracting a protective marking may be sent over the Internet without protection. Cryptographic protection should be considered if there are integrity, availability or authentication issues associated with the material.

1045. Notwithstanding the overall requirements for grades of cryptography laid down at **Chapter 23**, the following specific regulations apply to the requirements for the cryptographic protection of RESTRICTED material to be stored or forwarded using the Internet:

a. For electronic mail only, Baseline Grade (BG) cryptography that has been approved by CESG may be used to protect transmissions between appropriately cleared parties. This will normally involve the offline encryption of RESTRICTED attachment to be linked to an UNCLASSIFIED email, and is based upon an assumption of randomness, dilution, and short duration of storage. The use of mailboxes as "virtual repositories" (i.e. where they not regularly cleared) could potentially attract a requirement for a higher grade cryptography for any material stored therein. This is likely to be a particular issue for Web-based mail ;

b. For all other uses, including FTP server, "Virtual Drives", and remote backup services, InfoSy(Tech) should be contacted through the PSyA or DSSO as to the requirement.

1046. The use of the Internet for transmission of material protectively marked CONFIDENTIAL and above is currently prohibited.

Fax / Internet Mailboxes

1047. "FAX mailboxes" provided by Public Telephone Operators, and Internet based FAX services utilise "store and forward" technology without any assertion being possible as to the protection of data either in transmission or in storage. It is therefore not permitted to use such service for other than the transmission of UNCLASSIFIED material, and where a telephone number for either a PTO or Internet FAX mailbox is published, it must be clearly shown that it can only be used for the receipt of Unclassified material only. Fax/Internet mailboxes must comply with the requirements for facsimile machines laid down in this **Chapter 19**.

Internet Web Page Security

1048. MOD Websites are sites used for the promotion of officially sanctioned MOD business. All material published on a MOD Internet Website must be UNCLASSIFIED and conform to MOD's principles on disclosure of information. All material must conform to the principles of the Data Protection Act (DPA), and no material should be used where MOD does not own copyright.

1049. As mandated by JSP 440 (Defence Manual of Security), the publications of MOD information must receive approval from the appropriate authorities before release. These authorities are:

a. Directorate General Corporate Communications, within which sit the three Service Directorates of Corporate Communications (DCCs), for general MOD / Tri-service / Single-service items;

b. DDefSy(S&T), who have specific responsibilities for MOD on scientific and technical security matters, for material of a scientific or technical nature. DSTL has delegated powers in respect of its own material.

1050. The MOD and the single Services have well-established Websites, managed by the Directorate of Corporate Communication Services (DCCS) for the three Service DCCs. DSTL also maintains a number of Websites. In general, the MOD central Website oversees MOD and tri-service subjects and the Service Websites deal with single-Service subjects. DCCS also has a wider responsibility for MOD policy on the use of the Internet.

1051. All the Webmasters listed below welcome enquiries from anyone in MOD who wishes to publish information or provide services over the Internet:

a. General MOD/Tri-service - DCCS(IN)1/(IN)4 - 8633MB/70985MB

b. Royal Navy - DCCS (IN)5 - 78543MB

c. Army, DCCS (IN)2 / (IN)6 - 78431MB / 81618MB

d. RAF - Sgt RAF Internet - 78604MB

e. DSTL Webmaster - 01684 89 6000

1052. All MOD information must be published on a Web server with measures in place to provide Integrity and Availability protection. The unauthorised modification (e.g. defacement by a "hacker") is likely to attract a significant amount of unfavourable reaction from both the Press and, potentially, Parliament. Defacement and excessive downtime cause unacceptable damage both in terms of MOD's public image and its ability to provide services to the public.

1053. All Web servers hosting official MOD web sites, whether directly managed by Government or using DCCS contracted Servers, must therefore be Accredited by the relevant PSyA or the DSSO. In order to obtain accreditation it will be necessary for details of the security measures required to achieve security Accreditation to be enshrined in the security aspects letter agreed as part of the Contract. The Target of Accreditation will be at minimum :

a. Protection is afforded against tampering preferably through use of an approved firewall;

b. Any proxy servers facilities associated with the server(s) are to be configured to preclude their use by unauthorised personnel, and especially to prevent their use as Public Proxy Servers;

c. Configuration control procedures are in place, for instance to mitigate against the dangers of misuse of technologies such as Server Side Includes (SSI);

d. Management procedures are in place to re-validate this situation, in the form of Installation Vulnerability Reviews (IVR) which must be carried out at least once per month. Guidance on IVRs is given in **Chapter12**;

e. Management procedures are in place to detect and respond to any incidents affecting the web site. The preferred solution is for the site to incorporate firewall and router logging capable of immediately flagging up a likely intrusion to the Webmaster. Where the site is hosted by a contracted server, the security aspects letter must clearly state that it is the contractor's responsibility to monitor the firewall and router logging and to report incidents to the Webmaster at the earliest possible opportunity. Ideally, and where practicable, sites should also be directly or remotely accessible by a recognised MOD Monitoring and Reporting Centre (MRC) with 24 hr coverage.

f. Management procedures are in place to ensure that Sector Security staff and / or the JSyCC are notified of breaches of the security, integrity or availability of the site at the earliest opportunity. These procedures are also to detail the method by which the Website can be immediately taken off-line should this be directed by the Webmaster, Sector Security Authority or JSyCC. Where Websites are hosted by a contracted server, arrangements for notifying the Sector Security staff and / or JSyCC of breaches and for taking the site off-line are to be enshrined within the security aspects letter.

1054. Additionally, Security staffs may require Vulnerability Analysis (VA) to be carried out on a regular basis by either MOD or external organisations.

1055. As with e-mail addresses, it is important that only recognised, Official MOD Internet Domain Names are used for MOD Websites. The primary Websites for each Official domain will have Home Page links to a number of pages of global applicability for all MOD web sites, including aspects such a Copyright, Disclaimers, Acceptable Use, and a list of all recognised Official Domains, as well as Security issues.

1056. Links for security issues will include embedded email hotlinks, and alternative contact details, to permit Internet users to contact the MODCERT. It is therefore important that all official MOD Websites must provide a link back to one of these primary sites so that users can easily notify MODCERT if any vulnerabilities are detected on MOD Web servers.

1057. Where the author has a business requirement to publish directly to the Web server, either due to the volume of material or frequency of updates, it is possible to provide access to a sub-directory on the MOD server that can be accessed remotely. This requires prior approval by the MOD Webmaster.

1058. Unofficial Websites, such as those belonging to MOD clubs and societies, and private Websites established and maintained by individual staff are not to display any protectively marked material, or any official information, which is not for public view. Additionally, such Websites are to conform to the principles of the Data Protection Act (DPA) and other relevant legislation. The style and presentation of an unofficial or private Website should not give the impression that it is an officially sanctioned source of Defence information. Staff are advised to seek advice through the local ITSO if they are considering establishing a Website on a Defence or Government related topic. Any links to official MOD Websites must be approved by the Accreditor of that Website. Staff maintaining unofficial Websites are to ensure that these do not provide links to other Internet sites which might damage the public image of the MOD or cause it unnecessary embarrassment.

File Transfer Servers

1059. The security requirements for File Transfer (FTP) servers are broadly in line with those for Web Servers, especially in regard to Naming & Addressing and Accreditation.

Intranet Security

1060. An Intranet uses Internet technology and communication protocols on a network, or group of networks, which can be accessed only by authorised individuals. An Intranet can provide the full range of Internet type services and can be connected to the Internet through a controlled gateway. Intranets are systems and as such are subjected the policies set out in this manual. Some specific policy issues are highlighted below.

1061. The protective marking of e-mail messages and their attachments must be clearly displayed in accordance with the SyOPs for the system.

1062. There are constraints on the sending of e-mail to non-MOD addressees, or to MOD addressees via non-MOD controlled networks. Staff should consult the system's SyOPs for guidance and if necessary seek further advice from Security Staff.

1063. Staff proposing to establish an internal Website should consult the appropriate MOD Webmaster, who will provide advice on how to publish information. Material published on MODWEB and Web sites on Defence Intranets should carry the appropriate Protective Marking. In addition the first word of the HMTL title tag of Web each page must display the protective marking applicable to material on the page. MOD Webmasters will provide guidance on the procedures to be followed.

1064. Staff responsible for Websites should ensure that information held or created, does not as a result of aggregation warrant upgrade to a higher level of Protective Marking than that to which the Intranet is accredited.

1065. Additionally, Intranet Websites should provide Home Page hotlinks to standard pages covering aspects such a Copyright, Disclaimers, and Acceptable Use, as well as Security issues, in the same manner as Internet Web sites.

Precautions For Users Of The Internet

1066. The Internet is a hostile environment, and appropriate care should be taken when using Internet facilities to preserve Confidentiality, Integrity and Availability. Although this is not an exhaustive list of precautions, the following should be

considered, both when using the Internet for official purposes, and also when using the Internet by other means for personal purpose.

1067. Staff should be aware that some companies are offering Internet services specifically targeted at the armed forces. These companies may use official sounding names and offer the use of e-mail addresses with authentic military sounding domain names.

1068. Staff should be cautious in their dealings with companies offering Internet services, and in particular in any personal use of Internet features such as Chat Rooms. Reference to personal details, which could affect their personal security or reference to official activities or Service interests, should be avoided. Staff should be vigilant in their use of the Internet and if in doubt staff should verify the authenticity of those that they are dealing with. In any instances where personal internet contact expresses interest in service, departmental or political affairs, especially if this contact is from a foreign country, should be reported to the relevant unit security officer.

1069. Internet addresses of all kinds (e.g. mail name, Web server, File Transfer server) are easily "spoofed", and wherever possible some authentication should be used before trusting any information obtained from the Internet.

1070. For Web and File Transfer servers, it is preferable to use the IP address (dotted decimal format) when known rather than the eye readable domain name format. It is relatively easy either accidentally or deliberately to "poison" either the Domain Name Service (DNS), or a local Cache or Proxy, so that the information is sourced from a different server, which may have been subverted by an attacker.

1071. All files downloaded from or transmitted across the Internet should be checked for Malicious Software, in accordance with **Chapter 7**.

1072. All Internet users should be aware of the dangers of false information, known as "Hoaxes", many being passed on from the originator via reputable sources. Guidance on spotting hoaxes, and their close relatives Chain Letters, is given at **Chapter 11**.

1073. Internet users should be aware that:

a. External organisations will log accesses to their own Websites. This can identify both the user and the MOD. It may give further information to others for instance when an interest is expressed in a Newsgroup posting;

b. Normal legal rules apply to Internet activities;

c. Software, or other information, must not be downloaded unless the user has the right to copy it;

d. When acting in a personal capacity the reference to MOD in the user's e-mail address may infer responsibility for the user's opinions, given to a Newsgroup for example, to the MOD.

Improper Use Of The Internet

1074. Internet facilities provided by the MOD are for the pursuit of official business. Care must be taken that no messages are made publicly available that may be considered to be defamatory in any way and expose the sender or the MOD to retribution. In addition the use for personal advantage of Internet facilities provided by the MOD is not permitted, and may result in disciplinary action being taken against the user.

1075. The use of private internet facilities for official purposes on anything other than an occasional is discouraged, as if a business case exists (e.g. email exchange or file retrieval) for the use of Internet for official purposes, official CIS support should be procured and installed.

1076. The are facilities to monitor against misuse of the Internet. For example, some Internet Service Providers (ISPs) are able to provide audit trails. Commercially available software can also be used to limit access to a predefined range of Websites, e.g. pornographic sites.

1077. Types of prohibited activity are listed at **Annex B**. It is recommended that that a copy of Annex B is displayed next to terminals connected to the Internet.

ANNEX A TO
CHAPTER 10

SECURITY ISSUES FOR INTERNET SERVICES

The table below sets out some security issues and solutions for each of the major Internet services.

SERVICE	SECURITY ISSUE	SOLUTIONS
E-mail	Confidentiality and integrity of information may not be guaranteed A downloaded file could contain a virus	Use encryption techniques and digital signatures Use antivirus checking package to scan e-mail attachments
World Wide Web Pages	Unsuitable material may be downloaded A virus could be downloaded	Use software to limit access to predefined websites Use antivirus checking package that will scan downloaded files automatically
Information Exchange	The same concerns as e-mail but the potential impact could be greater	As for e-mail use encryption techniques and digital signatures
E-Commerce and Electronic Data Interchange	Integrity of information; guarantee of delivery to the intended recipient Confidentiality of information	Digital signatures Use encryption techniques

Protection for Information Exchange, E-Commerce and EDI can be provided by the use of a Value Added Network (VAN) as an alternative to the Internet

This page is intentionally left blank

ANNEX B TO CHAPTER 10

PROHIBITED USE OF INTERNET SERVICES

1. The use of Internet services in the following types of activities is specifically prohibited.

a. Illegal, fraudulent, or malicious activities.

b. Partisan political activity, political or religious lobbying or advocacy or activities on behalf of organisations having no connection with MOD.

c. Activities whose purposes are for personal or commercial financial gain. These activities may include chain letters, solicitations of business or services, sales of personal property.

d. Unauthorised fund-raising or similar activities, whether for commercial, personal, or charitable purposes.

e. Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.

f. Storing, processing, or distributing classified, proprietary, or other sensitive or for official use only information on a computer or network not explicitly approved for such processing, storage, or distribution.

g. Annoying or harassing another person, e.g., by sending or displaying uninvited e-mail of a personal nature or by using lewd or offensive language in an e-mail message.

h. Using another person's account or identity without his or her explicit permission, e.g., by forging e-mail.

i. Viewing, damaging, or deleting files or communications belonging to others without appropriate authorisation or permission.

j. Attempting to circumvent or defeat security or auditing systems without prior authorisation and other than as part of legitimate system testing or security research.

k. Obtaining, installing, storing, or using software obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

2. These activities may result in disciplinary action being taken against the person found misusing the Internet service for such purposes.

This page intentionally left blank

INCIDENT HANDLING (Including UNIRAS)

CHAPTER 11

INCIDENT HANDLING (INCLUDING UNIRAS)

Introduction And Scope

1101. The MOD has generic procedures for handling of many security incidents, in particular those of a terrorist or criminal nature, which are well established and simply codified.

1102. MOD's ability to respond and contain security incidents occurring within the Electronic Security Environment (ESE) of the MOD's CIS is fundamentally less easy to reduce to simple rules, as the nature of issues constituting an incident is less clearly delineated in these cases. The topic of incident handling is part of the wider issue of what is referred to in Allied groupings as Alert, Warning and Response (AWR), with details of the Warning policy within MOD being contained in **Chapter 2 Annex G**.

1103. Of particular note is the fact that even if such an event occurs on an UNCLASSIFIED or CL4 CIS, it may either directly or indirectly put Official information at risk, or have additional implications. A good illustration of such wider implications would be the unauthorised modification (e.g. defacement by a hacker) of an Official Website. This is a compromise of the integrity of Official Information, albeit UNCLASSIFIED, and is likely to attract a much greater amount of unfavourable reaction from both the Press and, potentially, Parliament, than the perceived impact of the incident in Confidentially terms would suggest.

1104. It is worth noting some terminology:

a. **Event –** An activity detected on CIS that may or may not be suspicious but affects CIS with a security relevance (e.g. an auditable activity like a failed log-on or a ICMP Echo Request ("PING") on a FireWall).

b. **Incident** – Any unauthorised Event affecting a CIS with security relevance (e.g. computer misuse) ;

c. **Intrusion** – Any set of actions that penetrate a system and attempt to compromise the Integrity, Confidentiality or Availability of a Security Barrier ;

d. **Attack** – Any Incident or Intrusion with Intent to cause and adverse affect on the Integrity, Confidentiality or Availability of the system.

1105. The terms CERT (Computer Emergency Response Team or CSIRT (Computer

Security Incident Response Team) are often colloquially used to describe the organisations responsible for this type of activity, but with wide variations on Terms of Reference. Within MOD therefore, the following terminology is to be used to describe elements of the role:

a. **ICC – Incident Coordination Centre**. A single focal point for the overall coordination of reporting and response to CIS security incidents within an organisation. Part of the role of the Joint Security Coordination Centre (JSyCC) is to provide the ICC for MOD;

b. **MRC – Monitoring and Reporting Centre.** Units roled to collate incident detection information and incident reports, and to onward disseminate this information to an ICC, via a higher level Co-ordinating MRC (CMRC) where relevant ;

c. **IRST – Incident Response Security Team.** Units roled to carry out technical response to CIS security incidents once so directed by an ICC.

1106. The term "MODCERT" may be encountered in certain publicly available documentation, and is the macro expression used in registrations with public for a (e.g. *FIRST* and *TI*) to cover the whole, distributed Incident Handling organisation within MOD.

1107. CIS Incidents may impact on some or all or the following Security services:

a. Confidentiality;

b. Integrity;

c. Availability.

1108. This Chapter describes the method which is to be used to report and respond to such security-relevant incidents or weakness, involving an initial fast response, followed by a more considered report.

Relationship To Law Enforcement

1109. It must be recognised that criminal activity, even where it involves CIS, is a matter for either the Ministry of Defence Police (MDP), Service Police, or other Law Enforcement agencies as appropriate. This Chapter therefore contains guidance for security staffs as to how to progress incidents reported to them, which are, or subsequently transpire to be, criminal activity. The nature of CIS installations makes it probable that a security rather than policing chain will be the initial point of contact for many such incidents.

Principles

1110. In order to appropriately handle all Information Security Incidents within Defence, it is important that the standardised procedures laid down in this Chapter are used in handling all incidents, however trivial they may seem initially, as failure to do so may jeopardise any investigation or other follow up action later discovered to be necessary.

National Policy

1111. The National Infrastructure Security Coordination Centre (NISCC) is a distributed organisation consisting of various central Government Departments including CESG, MOD/DSTL and the Police co-ordinated through the Cabinet Office. It is responsible for overall issues relating to Infrastructure Security, and in particular is charged with:

a. Developing effective working relationships with and between organisations that constitute and operate the Critical National Infrastructure (CNI);

b. Assessing and promulgating threats to, and vulnerabilities of, infrastructure assets, and promoting their protection, including offering alerts and advice on IT security matters such as viruses;

c. Acting as a central point of contact and response for Government organisations that are experiencing infrastructure security related problems, in particular Electronic Attack through UNIRAS (Unified Incident Reporting and Alert Scheme) system, which acts as the core Government CERT (GCERT).

1112. In addition to its role as NISCC contributing Department, the MOD is mandated to supply all relevant incident reports to the UNIRAS system, which acts both as a focal point for the Reporting and collating of security-relevant incidents or weaknesses, and for the promulgation of Briefings and Alerts as to Risks (both vulnerabilities / weakness or threats).

Privacy Of Data

1113. It is a condition of use of all Departmental CIS facilities is, and will continue to be, subject to monitoring, a fact which will normally be part of the User Security Instructions (USyI) or Security Operating Procedures (SyOPs) that users are expected to sign for as having read on a regular basis.

1114. All material held on MOD CIS equipment is deemed to be the property of the Department itself, and staff are reminded that, as a consequence, so-called private information held on any Departmental IT facility will not be afforded any special

protection and will be accessible to line management and investigating staff without notice.

Responsibilities

1115. **Joint Security Co-ordination Centre (JSyCC)** The JSyCC, as detailed at **Chapter 2**, has overall responsibility for co-ordination of all information security Alerting and Incidents Handling within MOD:

a. Co-ordinating the MOD contribution to NISCC;

b. Receiving and collating incident detection information;

c. Liasing with GCERT (UNIRAS), national and international CERT organisations;

d. Determining the nature of response required where incident would involve multiple MRCs and/or IRSTs, or where Defence Business or Operational factors may dictate a variant response ;

e. Arranging for, and supervising, any necessary external response where inappropriate to be carried out at unit or TLB level;

f. Carrying out any necessary post-incident analysis;

g. Co-ordination of awareness relating to Incident Handling.

1116. During working hours, incidents should normally be reported to JSyCC via the appropriate MRC where one exists. For significant issues that occur outside core working hours, the MOD maintains an Information Security Duty Officer (ISyDO), which is a role fulfilled by members of DDefSy or JSyCC staff, and is nominated to GCERT (UNIRAS) as the MOD's initial point of contact for all Information Security problems, and for OGDs reacting to Electronic Attack. Contact details for the JSyCC are given at **Annex A**, and the ISyDO can be reached through the JSyCC.

1117. **Monitoring and Reporting Centres** A number of Monitoring and Reporting Centres (MRCs) are identified to service the variety of units and formations that form MOD, contact details of which are provided at **Annex A**. The reporting chain for any incident will depend on the chain of command of the affected unit(s) and the nature of the incident, as some areas report to different MRCs for different categories of incident. Details of the correct reporting chain are provided at **Annex B**.

1118. **Incident Response Security Teams** A variety of Incident Response Security Team (IRST) functions are required to cover the breadth of incidents that may be encountered in defence, and the allocation of IRST resources to any incident where so required will be made by the MRC or JSyCC depending on the chain of command of

the affected unit(s), skills required, and IRST resource availability. Contact details for MOD IRST formations are given at **Annex A**, but it is stressed that units should not normally approach an IRST direct, but rather must report the incident first to the MRC or JSyCC and allow triage to be carried out.

Incident Cycle

1119. The Incident Response Cycle consist of the following phases:

a. Detection;

b. Triage;

c. Reporting;

d. Assessment;

e. Response;

f. Post-Analysis;

g. Remediation;

h. Closure.

1120. Responsibility for incident handling is shared between the System Operating Authority (SOA), Line Management, and the Security Staffs.

1121. Incident Handling procedures are part of the overall MOD AWR capability, with the Warning function, as described at **Annex G to Chapter 2**, being an element of the MOD Security Intelligence capability as defined at **Chapter 1 of JSP440 Vol 1**. The CIS A&W is a function performed by JSyCC on behalf of the Departmental Security Officer (DSO), and is intended to derive useful information from studying attempts to break through security controls. Although security intelligence is a matter which is principally the concern of security staffs and security units, all personnel in the MOD, whether Service or civilian, contribute to it by the prompt reporting of suspicious activity.

Detection

1122. Incidents will be detected by:

a. User Organisations;

b. CIS technical staffs;

c. Security staffs;

d. Internal Monitoring Capability (such as Intruder Detection Systems (IDS) or Real Time Monitoring (RTM));

e. MRCs.

1123. All MOD users are responsible for the reporting of any incident they discover through the appropriate chain of command.

Triage

1124. The process of Triage is that of an initial assessment of severity of any incident immediately after its detection, and deciding the nature of the immediate action required.

1125. It is the responsibility of the reporting Unit to make an initial Severity assessment, which is thereafter used to drive the Reporting and Response requirements, although the MRCs and/or JSyCC may have to subsequently review this assessment.

1126. There should normally be no need to carry out a specific Impact assessment, as the CIS should already have a Criticality Level (CL) assigned, as laid down at **Chapter 1 Annex A**. However, it is possible that the CL of a system may need to be varied to meet particular circumstances, for instance if it is supporting an Operational Deployment.

1127. Having made a severity assessment, reporting units should attempt to make an initial classification of the incident type, based upon the following taxonomy of CIS Security Incidents types derived from the UNIRAS system :

a. Breach of Security Policy:

(i) Transmission Violation;

(ii) Cryptosecurity Violation;

(iii) Mismarking of material;

(iv) Failure to observe security policy;

b. Hacking:

(i) Malicious Electronic Attack (MEA);

(ii) Electronic Attack (EA);

(iii) Other External;

(iii) Internal;

c. Malicious software:

(i) Virus;

(ii) Worm;

(iii) Trojan;

d. Misuse of resources;

e. Physical infiltration;

f. Theft;

g. Failure (hardware or software);

h. Personnel / Procedural error;

i. Personnel shortage;

j. Damage / disaster;

k. Fraud;

l. Bogus enquiry;

m. Hoaxes;

n. (Other).

1128. **Hoaxes**. The Internet is constantly being flooded with information about Malicious Software (e.g. computer viruses and Trojan Horses). However, interspersed among real Malicious Software warnings are hoaxes. Whilst these do not infect computer systems, they are still time consuming and costly to handle.

1129. All Malicious Software advisory information confirmed as originating from JSyCC (Vulnerability Warning Notices (VWN) and Vulnerability Rectification Directives (VRD)), as detailed at **Annex G to Chapter 2**, and from UNIRAS (Alerts and Briefings), may be regarded as Authoritative.

1130. All other warnings should be treated as provisional in the first instance. A Defence Information Assurance Notice (DIAN) is issued on a regular basis that lists

CIS related Hoaxes known to be circulating, along with a list of Internet Uniform Resource Locators (URLs) to Open Source references on known Hoaxes that are updated on a more dynamic basis.

1131. Only once these sources have been reviewed, to make an initial estimate of the nature of any non-authoritative warning received, should the appropriate escalation action be taken :

a. If no correlation to known Hoaxes is found, the relevant MRC, or JSyCC, should be informed as a matter of urgency so that any necessary action can be taken ;

b. If the warning has proved to be a Hoax, a UNIRAS report stating this should be submitted, along with any available details of the distribution path through which it was received.

Reporting

1132. It is mandatory for all Defence related CIS that all suspected, attempted, or actual incidents and weaknesses are to be reported to the JSyCC, via the relevant MRC where appropriate. Reporting of incidents is a vital part of the overall information security posture, as the trend analysis that can be performed at both a National (UNIRAS) and Departmental (JSyCC) level is used on an evolutionary basis to inform the risk management judgements.

1133. The potential impact of any occurrence, which will normally be the Criticality Level (CL) of the affected systems is used to determine the timescale in which the incident should be reported to the relevant MRC for upwards reporting to the JSyCC. Normal reporting timescales are detailed in the following table:

SYSTEM PROFILE	REPORTING REQUIREMENT	REPORTING POINT	REPORTING METHOD
CL1 or Category 1 systems, interconnected systems when attack (e.g. intrusions and malicious software) could propagate across the connection(s), and any incidents where Parliamentary, Press, or Public awareness is likely	Immediate	JSyCC / ISyDO, copied to to relevant MRC where appropriate	By telephone, followed by Immediate Signal or FAX.
CL2 systems	Within 4 hours	Relevant MRC, where available, or JSyCC	By telephone, followed by Immediate Signal or FAX.
CL3 systems	Within 1 working day		Priority Signal or FAX
CL4 systems	Within 2 working days		Routine Signal or FAX

1134. Special considerations also apply to certain types of incident, as detailed later in this Chapter.

1135. Early initial reports to Security Staffs allow a rapid judgement to be made as to the severity of the incident, and to minimise any delay likely to accrue in return to normal working whilst any required security response takes place. It will also provide them with an opportunity to provide specialist advice and guidance to the establishment at which the incident occurred.

1136. Care must be taken to assign an appropriate Protective Marking to all reports, and to use appropriate communications channels to meet this Protective Marking.

1137. Where a Protective Marking of CONFIDENTIAL or above is required for the initial report, if possible a sanitised RESTRICTED-INVESTIGATION summary should first be sent to JSyCC and any relevant MRC. An UNCLASSIFIED Codeword, to facilitate guarded discussions with over unprotected means will then be issued by JSyCC. JSyCC has various communications facilities available, with some being capable of handling both Voice and Data to TOP SECRET STRAP2, and STRAP3 or other strictly compartmented information can be passed by prior arrangement.

1138. A summary of the information required for initial reports is provided at **Annex C**, and some units may have access to software that will allow automatic submission of this information to the MRC / JSyCC.

1139. In all cases, a full report will also be required once the Incident has been closed, protectively marked according to its content. In all cases where Criminal or Security investigation has occurred, the report should be marked RESTRICTED-INVESTIGATION at minimum.

1140. The final report should normally be completed by the Unit(s) detecting the Incident, and is to be forwarded to JSyCC, via the MRC where appropriate. An electronic version is available for online completion on some MOD Intranets, which will allows the updating of the record created for the initial report.

1141. If in doubt as to which form to complete, contact the appropriate MRC or the JSyCC. On no account is the vendor of a faulty product to be informed without first seeking the advice of the JSyCC.

1142. **Major Breaches**. Certain categories of incident will require either a more rapid or in-depth investigation than that indicated by CL alone, including in some cases a Counter Intelligence (CI) investigation. Unit(s) detecting the Incident, or the MRC, should **immediately** contact the JSyCC or ISyDO for direction in **all instances** of:

a. Actual or suspected compromise of systems handling Category 1 material in accordance with **Chapter 2 of JSP 440 Vol 1**;

b. Actual or suspected compromise of systems handling STRAP or other Compartmented material in accordance with **Chapter 8 of JSP 440 Vol 5**;

c. Actual or suspected compromise of systems handling IDO (e.g. NATO) material;

d. Actual or suspected compromise of cryptosystems;

e. Actual or suspected instances of system Intrusions (hacking**), including Electronic Attack /Malicious Electronic Attack (MEA);**

f. Any cases of serious, ongoing or unexplained breaches of security which cannot be adequately categorised.

1143. Major Security Breaches must as a minimum be handled as RESTRICTED-INVESTIGATION.

Security Breaches

1144. **Breach of Security Policy**. Where a breach of National or Departmental security policy has occurred, the Head of Establishment is responsible for ensuring that, in addition to any action required by this Chapter, appropriate personnel security action is also taken.

1145. **Cryptosecurity Breaches**. More details on this topic are provided at **Chapter 23.**

1146. **Transmission Violations**. More details on this topic are provided at **Chapter 18 (Telephony), Chapter 19 (Facsimile), Chapter 23 (Cryptosystems), or Chapter 25 (Messaging Systems).**

Hacking

1147. **Electronic Attack** Electronic attack is defined for UK Government as gaining unauthorised electronic access to a CIS in order to exploit them for unauthorised or intelligence purposes, or, in the case of MEA, to disrupt their operation. This is often referred to in Allied documents as a Computer Network Exploitation (CNE) or Computer Network Attack (CNA).

1148. At the simplest the defacement of an Internet or Intranet Web Site is *prima facie* evidence that a MEA has occurred, although the fact that an intrusion has occurred does not in itself mean that there has been an EA or MEA.

1149. Responsibility for EA Response (EAR) is coordinated across HMG by the NISCC under the auspices of the NISCC Advisory Group (NAG), on which JSyCC represents MOD.

1150. Outside of Defence, the *de facto* method of assigning EAR focal points for Internet domains lies with the Federation of Incident Response and Security Teams (FIRST) organisation. MOD, through DCSA, is registered via Nominet as the owner of the Internet Class A *25.x.x.x* domain (*'.mod.uk'* /*'.mil.uk'*), the Class B domain *146.80.x.x* (*'dstl.gov.uk'/* '*dera.gov.uk'/ 'dera.hmg.gb'*) operated by DSTL, and Class C domain *205.136.x.x* (*'moduk.org'/ 'bdsw.org')* operated by BDS(W). MODCERT is registered with FIRST as being the competent authority responsible for these domains, with JSyCC being designated as the focal point for all communications with other FIRST Teams.

1151. Additionally, there are a number of Legacy Internet Websites and mail addresses used by MOD without this naming scheme, most of which will be operated by ISPs on behalf of MOD, which have not as yet been migrated to an Official domain. It is important that the JSyCC, as the MOD FIRST point of contact, is informed immediately of incidents affect such CIS.

1152. The '*.mil*' Internet Top Level Domain (TLD) and its associated sub-domains are not related to UK MOD, but rather to the US DOD. However, as JSyCC has cooperation agreements with FIRST, Allies, Other Government Departments (OGD), and commercial entities that constitute the Critical National Infrastructure (CNI), incidents affecting any TLD or High Level Domains (HLD) relevant to such partners should be notified to JSyCC who will make sure the appropriate authorities are informed.

1153. **Other External Hacking**. This incident type covers the majority of Intrusions that make the attention of the News Media, and will include the activities of *Hobby Hackers, Hacktivists* and *Script Kiddies*. Regardless of apparent motive, any Intrusion will be regarded as *prima facie* evidence of a criminal activity, typically of the Computer Misuse Act.

1154. **Internal Hacking**. The nature of what constitutes Internal Hacker is difficult to define, as it often will not technically constitute an Intrusion. Typical examples would be privilege abuse (e.g. unauthorised modification of shared files), or unauthorised privilege escalation (often referred to as a root compromise from the UNIX heritage).

1155. In all cases where an external intrusion into MOD networks has occurred, part of the investigation will normally require a "trace back" in an attempt to ascertain the origin of the intrusion.

1156. Active tracing techniques into other domains can be considered by that domain's owners as an intrusion in their own right, and could therefore be regarded as

illegal, or even an EA / MEA. Active tracing techniques must not therefore be used without prior sanction by JSyCC.

1157. In all such cases, the details of the source domain obtained from passive tracing should be supplied to JSyCC. Where the source is believed to be an Internet Service Provider (ISP), MRCs may contact the ISP's Abuse or Security teams direct to pursue the matter, ensuring that JSyCC, as the MOD FIRST representative, is copied all information passed to such ISPs.

System Weaknesses

1158. IT systems often contain faults which come to light only after extensive use, or when unusual conditions enable them to be discovered. Occasionally, these faults are already known to the manufacturer or supplier; often, they are not.

1159. In order that the appropriate security and/or technical authorities can react to make systems less flawed or susceptible to misuse, all possible security weaknesses or faults are to be reported, through the MRC where appropriate, to the JSyCC.

1160. Even a problem discovered on an UNCLASSIFIED or CL4 computer may have implications for a Protectively Marked or more critical system running on similar hardware or software, or using similar procedures. Moreover, systems may have an operational significance additional to the level of protection required by the data held.

Disciplinary And Criminal Considerations

1161. In addition to Information Security concerns, CIS Incidents may also involve disciplinary and criminal considerations.

1162. **Malicious Damage and Theft.** Deliberate damage to, and theft of, MOD CIS assets are clear indications of a criminal act having occurred, and as such either the Ministry of Defence Police (MDP) or Service Police, as appropriate, must be contacted. In cases where a serious breach of National Security has also occurred (i.e. Category 1 material is involved), JSyCC must also be informed immediately.

1163. Reporting Units or the MRC are responsible for ensuring that an UNIRAS Incident Report is raised in addition to any report supplied to the Police.

1164. **Physical infiltration.** The physical infiltration of a MOD site by unauthorised persons should be dealt with by either local security staffs, through the MDP or Service Police as appropriate, as laid down in **JSP440 Volume 1**. Any collateral incidents (e.g. Theft) should, however, be assessed against the guidance in this Chapter, and reporting Units or the MRC are responsible for ensuring that an UNIRAS and/or SIRS Incident Report is raised in addition to any report supplied to the Police.

1165. **Misuse of resources.** Improper use of MOD CIS facilities comprises a range of activities and behaviour, contrary to Security Operating Procedures (SyOPs), sound practice, or commonsense, and may be defined as "the deliberate, inappropriate or illegal use of any part of the MOD's CIS facilities". **Chapter 1** contains a summary of many of the legal constraints on the use of CIS, including the Data Protection Act (DPA), the Computer Misuse Act (CMA), and the Copyright, Designs and Patents Act (CDPA).

1166. The list of prohibited use of MOD CIS that has been published included a variety of activities that fall without the remit of security, but those common incidents types likely to be brought to the attention of security staffs include:

a. The sending of offensive/abusive or excessive (spam) e-mail;

b. The use of e-mail or other facilities for private and commercial purposes;

c. The use of anything of a sexual nature as desktop `wallpaper';

d. The importation, distribution and use of unauthorised software (including graphics files, text files, computer games and many other variants);

e. The accessing, without permission, of non work-related Internet sites, typically for Downloading or Forwarding of Indecent Material.

1167. Personnel are individually responsible for using MOD CIS in an appropriate and lawfully effective manner. All personnel have a responsibility to report any suspected cases of CIS misuse which they encounter.

1168. Where criminal activity is suspected, the Ministry of Defence Police (MDP) or Service Police as appropriate should be contacted immediately. Reporting Units or the MRC are responsible for ensuring that an UNIRAS Incident Report is raised in addition to any report supplied to the Police.

1169. When cases of misuse of resources are suspected, but no clear indication of criminal activity exists, care should be taken not to take any action that might later prejudice a criminal investigation, and guidance on preservation of evidence is given at **Annex D**. **Before taking an action**, Security Staffs should immediately contact JSyCC, or, for urgent matters outside of core hours, the MOD Information Security Duty Officer (ISyDO), who will advise on appropriate action to be taken.

1170. **Malicious software.** Although any infestation by Malicious Software is *prima facie* evidence of a breach of the Computer Misuse Act (CMA), only in cases where the infestation appears to have been deliberately and specifically targeted at, or to have originated within, MOD, will a Criminal Investigation, involving MDP or Service

Police, normally be required. **Chapter 7** provides detailed advice on this topic. Reporting Units or the MRC are responsible for ensuring that an UNIRAS Incident Report is raised in addition to any report supplied to the Police.

Assessment

1171. Upon receipt of the initial report, the MRC or JSyCC will issue an Incident Report Occurrence Number (IRON) that is used to track the incident for the rest of its existence, until an Incident Report Closure Number (IRCN) is issued. Sectors may also allocate their own reference number (e.g. RAF Police case number) for internal use, but the IRON must be included for all external communications.

1172. In the case of Major Security Breaches, an UNCLASSIFIED Codeword will have been allocated to the Incident, and in such cases the mapping of Codeword to IRON must be protected to at least RESTRICTED-INVESTIGATION until the incident is finally closed.

1173. Based upon the Report made by reporting Unit(s), the MRC or JSyCC / ISyDO will make an assessment of the type of response required. A number of different types of Response have been identified, as defined in the table below. If it is felt that the Incident may fall into more than one of these types, the response actions should be carried out in strict accordance with the Priority sequence assigned below so as not to prejudice any follow up action that may be required.

PRIORITY	INCIDENT TYPE	RESPONSE TYPE	RESPONSE TIME
1	Offensive IW	Operational	Immediate
2	Other EA or MEA	Security	
3	Serious Breach	Security	
4	Criminal	Police	
5	Technical Infosec	Technical	Dependent on Criticality Level (CL)
6	Other Incidents	Unit	

1174. Where the response required is dependent on Criticality Level (CL) of the CIS affected, the following metric should be applied:

CRITICALITY LEVEL	RESPONSE TIME	COORDINATION BY
CL1	Immediate	JSyCC / ISyDO
CL2	Within 8 hours	MRC Incident Manager, where available, or JSyCC
CL3	Within 1 working day	
CL4	To Unit Priorities	Unit Security Staffs

Response

1175. Before commencing any detailed investigation or other form of response, an appropriate Incident Reporting action as laid at paragraphs 1134 - 1146 must be carried

out. There may be wider implications that the reporter is not aware of that will require the MRC, JSyCC or ISyDO to direct a different course of action than the local Unit may otherwise have intended.

1176. **Security Investigations**. Investigations into Major breaches and compromises of CIS, other than those that are Police matters, will be performed by an Investigation Team under the remit of the Accreditor of the system. Where the incidents affect systems under the jurisdiction of more than one Accreditor, the JSyCC will co-ordinate. Requirements for security investigators are laid down at **JSP440 Volume 1 Chapter 2**.

1177. Local Security Staffs normally perform minor breaches investigations on behalf of the Head of Establishment.

1178. **Computer based Forensics** Failure to comply with the requirements laid down in the Police and Criminal Evidence (PACE) Act may jeopardise any future prosecution.

1179. In cases where no criminal activity is suspected, but where there is a perceived need for Computer-based evidence for other purposes, then the JSyCC should be contacted who will be able to direct units to either the MDP Computer Crime and Examination Unit (CCEU), or to Service Police units having access to Computer Forensic capability, as appropriate.

1180. **Indecent or Obscene Material**. Where material that may be considered to be indecent or obscene is encountered on a system, **all local investigations must cease** until advice has been obtained from the either the MDP CCEU or Service Police as appropriate.

1181. **Unit Response**. Large systems and networks should have documented procedures on managing incidents, in the form of an Incident Response Plan as defined at **Chapter 3**. This should include details as to how levels of degradation are to be managed, if it is required for operational reasons. For networks and interconnected systems it may be necessary to have a form of Service Level Agreement to cover circumstances, which could include whether to:

a. Keep the system operational and be managed in conjunction with the appropriate extramural support;

b. Sever interconnections with other systems;

c. Take the system down.

Post-Analysis

1182. Once the initial Incident Response has been carried out, the final incident report must be produced by the unit or formation affected, using the IRON already. Wherever possible these reports should be submitted to the relevant MRC or JSyCC as appropriate using the MODAWR feeder database system where available, but legacy reporting techniques using previous UNIRAS database formats (*Access* or *Excel*), or the GS490 series hardcopy forms, will be accepted until 1st July 2002.

1183. Such reports will be added to databases held by JSyCC and other agencies (including UNIRAS), and used both to direct follow up activity if necessary, and Trend Analysis to inform the wider view on Threats, Vulnerabilities and Risks. The JSyCC will disseminate investigative reports to other Security staffs as and where applicable.

1184. For all instances of EA and MEA, and some other technical incidents, a more in-depth analysis of information relating to an Incident may also be appropriate, which will typically involve the detailed examination of ESE Accounting and Audit records. Unit(s) and/or the MRC should provide any assistance requested by JSyCC in this respect, which may be used to direct any Remediation required.

1185. The Commanding Officer or Head of Establishment is responsible for ensuring that appropriate personnel security action is taken in instances where MOD staff or contractors have been involved in either misusing CIS resources, or conducting criminal activity. This would normally require an Aftercare Incident Report (AIR) being raised to the Defence Vetting Agency (DVA).

Remediation

1186. Once any Incident Response has been completed, it is the affected Unit(s) responsibility to arrange for any required remediation to the CIS(s) affected. In some cases this will require re-accreditation of the system, as laid down at **Chapter 2**.

Closure

1187. No Incident may be considered closed until an Incident Report Closure Number (IRCN) has been obtained from the MRC or JSyCC, which will not be issued until all required Post Analysis and Remediation has been completed.

CIS Support

1188 The Defence CIS architecture to support the overall MODAWR capability, and its linkages to NISCC and Allies, is currently under development, which will include the provision of a hardened MOD AWR Bearer Network (MABN) to provide an out of band link between the core formation involved in these activities.

1189. In the interim, it is essential that all MRCs and IRSTs have access as a minimum to mail services on both the Internet and RLI, have a valid Signal Message Address with appropriate SIC distribution configured for *Y3A* and *Y3B*, and have IT equipment to run the distributed MODAWR database that is being produce to supplant the previous UNIRAS system. Any local IT initiatives that include Incident Handling aspects, such as Fault Ticketing systems, should as a minimum support data import and export in line with the latest version of the Internet Engineering Task Force's (IETF) *Incident Object Description and Exchange Format* (IODEF), which was *RFC3067* at time of the publication of this document.

Authority

1190. In cases where there is a significant operational imperative for a CIS to be operated where its security is non-compliant with national and departmental baseline requirements, for instance when an incident has occurred, Risk Management principles permit senior staff, of at least 2* rank, to accept the risk of continuing its operation contrary to the advice from an MRC or JSyCC, provided that :

a The material processed on the system does not fall within Category 1, as laid down in **Volume 1** ;

b The risk is constrained solely to the risk acceptor's management domain.

1191. The nature of modern CIS, and in particular the degree of interconnectivity, will however mean that a security incident or weakness occurring within one management domain may well have adverse implications for the wider Defence community. In such cases, the JSyCC may, in consultation with ACDS(Ops) and/or DG Info, need to direct either the cessation of processing on any affected CIS installation, or its isolation from other domains, whilst any Incident Response and Remediation takes place.

This page intentionally left blank.

ANNEX A TO

CHAPTER 11

MOD INCIDENT HANDLING UNITS

1. The MOD Alert, Warning and Response (AWR) capability, colloquially referred to as the MODCERT (Computer Emergency Response Team), is a virtual or distributed organisation consisting of one overall Incident Co-ordination Centre (ICC) that serves as the focal point for the department, and a number of Monitoring and Reporting Centres (MRCs) and Incident Response Security Teams (IRSTs) which service distinct communities within the department.

2. The table overleaf gives contact details for units assigned to ICC, MRC or IRST roles at the time of publication of this Volume. An updated version of the table can be found on the Joint Security Co-ordination Centre website on the MOD Intranet.

3. The allocation of the UNIRAS sub-department numbers used in the table overleaf are controlled by JSyCC, with the exception of the following ranges where a sub-delegation has been granted, where any additional numbers issued must be notified to JSyCC:

Range	Area of Responsibility	Allocating Authority
0100-0199	CJO	PJHQ(UK) J2X
1000-1099	Centre TLB	CB(Sy)
1100-1199	DPA	DPA PSyA
1200-1299	DLO	DLO PSyA
1300-1399	DSTL	DSTL PSyA
1400-1499	Met Office	Met Office PSyA
2000-2399	RN TLBs	DNSyICP
2400-2499	UKHO	UKHO PSyA
3000-3299	Army TLBs	Land G2Sy(Info)
4000-4299	RAF TLBs	SyCIS(RAF)

MOD Incident Handling Units								
Unit Type	**UNIRAS Number**	**Title**	**Telephone Contacts**				**Email**	
			Core Hours	**Duty Officer**	**Facsimile**	**Messages (SIC Y3B)**	**Intranet**	**Internet**
ICC	47-0001	Joint Security Co-ordination Centre (JSyCC)	020-7218-0117	020-7218-0117	020-7218-1165	MODUK	JSyCC	cert@cert.mod.uk
MRC	47-0002	MDP CIR	01371-85-4444	01371-85-4444	01371-85-4030	CCMDP WETHERSFIELD	MDP CIR	t.b.a.
IRST	47-0003	MDP CEU	01371-85-4480	01371-85-4444	01371-85-4030	CCMDP WETHERSFIELD	t.b.a.	t.b.a.
MRC	47-0100	PJHQ(UK) J2 CI/Sy	38027NW	Contact ISyDO	38019NW	PJHQUK	t.b.a.	t.b.a.
MRC	47-0101	BF Cyprus	5185 CYP	Contact ISyDO	5144 CYP	t.b.a.	t.b.a.	t.b.a.
MRC	47-0102	BF Falkland Islands	6556 MPA	Contact ISyDO	6735 MPA	t.b.a.	t.b.a.	t.b.a.
MRC	47-0103	BF Gibraltar	5428 GIB	Contact ISyDO	4513 GIB	t.b.a.	t.b.a.	t.b.a.
MRC	47-0110	PJHQ Deployed Formations	01923-8-46145	Contact ISyDO	01923-8-46013	PJHQUK	t.b.a.	t.b.a.
MRC	47-0200	NATO CIRC CC	Contact JSyCC	Contact ISyDO	t.b.a.	t.b.a.	t.b.a.	t.b.a.
IRST	47-0201	NC3A	Contact JSyCC	Contact ISyDO	t.b.a.	t.b.a.	t.b.a.	t.b.a.
IRST	47-0900	CESG Consultancy Support	Contact JSyCC	Contact ISyDO	t.b.a.	t.b.a.	t.b.a.	t.b.a.
IRST	47-0901	MODCERT Contract Support	Contact JSyCC	Contact ISyDO	t.b.a.	t.b.a.	t.b.a.	t.b.a.
MRC	47-1000	CB(Sy)	020-7218-2857	Contact ISyDO	t.b.a.	t.b.a.	t.b.a.	t.b.a.
MRC	47-1001	CITSO(NA)	+1-202-588-6848	Contact ISyDO	+1-202-588-7888	t.b.a.	t.b.a.	t.b.a.
MRC	47-1003	DIS	020-7218-5105	Contact ISyDO	020-7218-7210	t.b.a.	t.b.a.	t.b.a.
MRC	47-1100	DPA Sy	0117-91-30622	Contact ISyDO	t.b.a.	t.b.a.	t.b.a.	t.b.a.
MRC	47-1200	DLOHQ Sy	01225-4-68941	Contact ISyDO	t.b.a.	t.b.a.	t.b.a.	t.b.a.

MOD Incident Handling Units								
Unit Type	**UNIRAS Number**	**Title**	**Telephone Contacts**				**Email**	
			Core Hours	**Duty Officer**	**Facsimile**	**Messages (SIC Y3B)**	**Intranet**	**Internet**
MRC	47-1201	DCSA GOSCC	7560RM	7556RM	7586RM	t.b.a.	t.b.a.	t.b.a.
MRC	47-1300	DSTL PSyA	023-92-33-7327	Contact ISyDO	t.b.a.	t.b.a.	t.b.a.	t.b.a.
MRC	47-1301	DSTL NOC	01684-89-6000	Contact ISyDO	01684-89-5700	t.b.a.	t.b.a.	t.b.a.
IRST	47-1302	*Qinetiq* Consultancy Support	Contact JSyCC	Contact ISyDO	t.b.a.	t.b.a.	t.b.a.	t.b.a.
MRC	47-1400	Met Office	t.b.a.	t.b.a.	t.b.a.	t.b.a.	t.b.a.	t.b.a.
MRC	47-2000	DNSYICP	27135 PY	Contact ISyDO	27127PY	t.b.a.	t.b.a.	t.b.a.
IRST	47-2001	RN SIB	23131 PY	Contact ISyDO	23193PY	t.b.a.	t.b.a.	t.b.a.
IRST	47-2002	CITSS(RN)	25586 PY	Contact ISyDO	27127PY	t.b.a.	t.b.a.	t.b.a.
IRST	47-2300	UKHO	t.b.a.	t.b.a.	t.b.a.	t.b.a.	t.b.a.	t.b.a.
MRC	47-3000	Land G2 Sy(Info)	3875/3695SM	3673SM	2800SM	t.b.a.	t.b.a.	t.b.a.
MRC	47-3001	PM(A)	94321 3659	Contact ISyDO	94321 5658	t.b.a.	t.b.a.	t.b.a.
MRC	47-3002	UKSC(G) / G2Sy(Info)	2764JHQ	Contact ISyDO	2769JHQ	t.b.a.	t.b.a.	t.b.a.
MRC	47-3003	HQNI / G3Sy(Info)	42588LIS	Contact ISyDO	41822LIS	t.b.a.	t.b.a.	t.b.a.
IRST	47-3004	AISU	94649 2416	0771 972763	96649 2420	t.b.a.	t.b.a.	t.b.a.
MRC	47-4000	SYCIS(RAF)	95331 6687	95331 6670	01480 458623	t.b.a.	t.b.a.	t.b.a.
MRC	47-4001	RAF P&SS (UK)	95381 8234	95381 8220	01462 817144	t.b.a.	t.b.a.	t.b.a.
MRC	47-4002	RAF IPOC	95712-7499	Contact ISyDO	t.b.a.	t.b.a.	t.b.a.	t.b.a.
IRST	47-4003	591SU	95712-7499	Contact ISyDO	t.b.a.	t.b.a.	t.b.a.	t.b.a.

This page intentionally left blank

ANNEX B TO

CHAPTER 11

MOD INITIAL INCIDENT REPORTING POINTS

1. The MOD Alert, Warning and Response (AWR) capability, colloquially referred to as the MODCERT (Computer Emergency Response Team), is a virtual or distributed organisation consisting of one overall Incident Co-ordination Centre (ICC) that serves as the focal point for the department, and a number of Monitoring and Reporting Centres (MRCs) and Incident Response Security Teams (IRSTs) which service distinct communities within the department.

2. Due to the variety of incident types covered by MOD and UNIRAS reporting requirements, the reporting chain can vary depending on the type of incident encountered.

3. The table overleaf gives assignment of reporting points to the units assigned to ICC, MRC or IRST roles for the standard incident categories. This assignment was current at the time of publication of this Volume, and an updated version of the table can be found on the Joint Security Co-ordination Centre website on the MOD Intranet.

MOD Initial Incident Reporting Points														(using UNIRAS "sub-department" designator from **Annex A**)
Area of Responsibility affected by Incident	**Breach of Security Policy**	**Hacking including EA / MEA**	**Malicious Software**	**Misuse Of Resources**	**Physical Infiltration**	**Theft**	**Hardware or Software Failure**	**Personnel / Procedural Error**	**Personnel Shortage**	**Damage or Disaster**	**Fraud**	**Bogus Enquiry**	**Hoax**	**Other**
Impact pan-MOD or on OGD or Allies, CL1 or Category 1, publicly known	47-0001	47-0001	47-0001	47-0001	47-0001	47-0002	47-0001	47-0001	47-0001	47-0001	47-0002	47-0001	47-0001	47-0001
DCSA Networks	47-1201	47-1201	47-1201	47-1201	47-1201	47-0002	47-1201	47-1201	47-1201	47-1201	47-0002	47-1201	47-1201	47-1201
Overseas garrisons, current deployments, CJO TLB	47-0100	47-0100	47-0100	47-0100	47-0100	47-0100	47-0100	47-0100	47-0100	47-0100	47-0100	47-0100	47-0100	47-0100
Northern Ireland units	47-3003	47-3003	47-3003	47-3003	47-3003	47-3003	47-3003	47-3003	47-3003	47-3003	47-3003	47-3003	47-3003	47-3003
Units in Northwest Europe including UKSC(G)	47-3002	47-3002	47-3002	47-3002	47-3002	47-3002	47-3002	47-3002	47-3002	47-3002	47-3002	47-3002	47-3002	47-3002
Units based in North America	47-1001	47-1001	47-1001	47-1001	47-1001	47-1001	47-1001	47-1001	47-1001	47-1001	47-1001	47-1001	47-1001	47-1001

Area of Responsibility affected by Incident	Breach of Security Policy	Hacking including EA / MEA	Malicious Software	Misuse Of Resources	Physical Infiltration	Theft	Hardware or Software Failure	Personnel / Procedural Error	Personnel Shortage	Damage or Disaster	Fraud	Bogus Enquiry	Hoax	Other
FLEET & 2SLCNH TLBs	47-2000	47-2000	47-2000	47-2000	47-2000	47-2001	47-2000	47-2000	47-2000	47-2000	47-2001	47-2000	47-2000	47-2000
LAND & AG TLBs	47-3000	47-3000	47-3000	47-3000	47-3000	47-3000	47-3000	47-3001	47-3000	47-3000	47-3001	47-3000	47-3000	47-3000
STC and PTC TLBs	47-4000	47-4000	47-4000	47-4000	47-4000	47-4000	47-4000	47-4001	47-4000	47-4000	47-4001	47-4000	47-4000	47-4000
2nd PUS	47-1000	47-1000	47-1000	47-1000	47-1000	47-0002	47-1000	47-1000	47-1000	47-1000	47-0002	47-1000	47-1000	47-1000
DPA TLB	47-1100	47-1100	47-1100	47-1100	47-1100	47-0002	47-1100	47-1100	47-1100	47-1100	47-0002	47-1100	47-1100	47-1100
DLO TLB and DARA Trading Fund	47-1200	47-1200	47-1200	47-1200	47-1200	47-0002	47-1200	47-1200	47-1200	47-1200	47-0002	47-1200	47-1200	47-1200
DSTL Trading Fund	47-1300	47-1300	47-1300	47-1300	47-1300	47-0002	47-1300	47-1300	47-1300	47-1300	47-0002	47-1300	47-1300	47-1300
UKHO Trading Fund	47-2300	47-2300	47-2300	47-2300	47-2300	47-0002	47-2300	47-2300	47-2300	47-2300	47-0002	47-2300	47-2300	47-2300
Met Office Trading Fund	47-1400	47-1400	47-1400	47-1400	47-1400	47-0002	47-1400	47-1400	47-1400	47-1400	47-0002	47-1400	47-1400	47-1400

This page intentionally left blank.

ANNEX C TO

CHAPTER 11

INITIAL INCIDENT DETECTION REPORTS INFORMATION REQUIRED

1. Protective Marking

According to nature of incident. For all Major Breaches or Criminal Matters, this should be at least RESTRICTED-INVESTIGATION.

2. Description of System Affected, to include :

(i) System Name ;

(ii) Location(s) ;

(iii) Protective Marking ;

(iv) Criticality Level (CL) ;

(v) System Manager or other relevant point of contact.

3. Summary of Incident

This is to include the details of any IP address ranges from an attack may have originated, or names of any malicious software detected.

4. Damage Assessment

The reporting unit must carry out an initial assessment of possible damage to Confidentiality, Integrity and Availability of the system and the information, along with an assessment as to whether the incident was deliberate or accidental. It is not sufficient merely to describe possible damage as 'serious' without explanation.

5. Brief Description

The reporting unit must attempt an initial assessment to summarise how or why the incident is believed to have occurred.

6. Immediate Action Taken

This is to include confirmation that all units or organisations known by the originator to be interested in, or affected by, the attack or infection have been, or are about to be, informed, and steps that have been, or are about to be, taken to preserve evidence.

This page intentionally left blank.

ANNEX D TO

CHAPTER 11

PRESERVATION OF EVIDENCE AND CHAIN OF CUSTODY

1. **Secure the Site of Evidence**

- Constrain access to the site(s) affected until the evidence has been collected, both to maintain integrity and prevent damage (eg overwrite, physical damage or even arson !)

2. **Physical Evidence**

- Recognition and location of where acquired

- Equipments types involved

- Floor plan for major installations [Graph paper; tape measure]

- System schematic for distributed systems indicating locations affected

- Support with photographs where useful [35mm camera; flash]

3. **Collect Evidence**

- Ensure that no forensic tests (fingerprints ...) are required before attempting to collect evidence

- Magnetic evidence should include details of collection technique(ps)

- Printed evidence has attractions if to be used in Court

- Handwritten documents, including hand-amended listings (eg for logic bombs ...) , MUST NOT BE ALTERED. Pin together, photocopy for identification purposes, and seal.

4. **Identify Evidence**

- Unique identification marks should be placed on all media EXCEPT HANDWRITTEN EVIDENCE

- Include where practicable details of the incident (file reference(ps), type of incident, location, unit/branch, and investigator(ps) names)

- Open reel tape can be marked with permanent marker on the dull side - the first 15-20 feet before the BOT contains NOTHING of use to a system [Permanent marker]

- Etch information on bottom of metal disc packs [Carbide tipped metal marker]

- Take car as magnetic media are very sensitive to dust, fingerprints, and physical damage, all of which could destroy the evidence

- Printouts should be marked with a permanent marker pen. Handwritten evidence should be marked on the photocopies held with the (sealed) originals

5. **Description of the Evidence**

- List all evidence, including extended details where these are not practical to mark on the evidence itself

- Detail format of evidence, and where applicable the equipment requirements to interrogate the data contained

6. **Remove the Evidence**

- Once the collection and collation has been completed, the evidence should be removed from the site of the incident ass soon as possible.

- If part of an installation represents evidence, and cannot be removed, and/or is required for use, seek legal advice as to how this can be secured if needed for future evidential purposes.

7. **Secure the Evidence**

- The storage should be secured from unauthorized access. It should ideally be "off site" from the area affected.

- Where practicable, seal the evidence in tamper proof coverings appropriately signed. Affix easily readable labels [Evidence bags]

- Magnetic media should be secured inside a hard covering to prevent damage.

8. **Preserve the evidence**

- Ascertain the specific storage requirements for each type of evidence to maintain its integrity. Consult manufacturers guides where necessary.

- Thermal transfer printouts should be kept away from direct light

- All printout should be stored flat, between binders, and away from strong light.

- Unless unavoidable, do not burst continuous feed paper.

- Ensure loose paper is page numbered

- Discs should be stored away from dust

- Media should be stored away from magnetic fields, at 40-90F / 20-80%RH. Shelf life is normally 3 years without rewriting.

9. **Maintain Access Control**

- The storage selected should be limited in access to the Investigator(ps) and other relevant personnel.

- A record should be kept, in chronological order, of all persons having access to the evidence once labelled

10. **Examination of Evidence**

- Use photocopies for working documents

- Number working sets so these can be identified

- Only photocopies of evidence should be returned too active use before the investigation is completed

- Written evidence may need to be examined by a handwriting expert, especially for coding sheets and amended listings when trying to apportion the personnel responsible for various sections.

- Forensic advice may be required to ascertain the order in which documents were written. This will require access to the originals, which must be controlled and recorded.

This page intentionally left blank.

COMPLIANCE ACTIVITIES

This page intentionally left blank.

CHAPTER 12

COMPLIANCE ACTIVITIES

General

1201. Compliance is a general term to describe activities which ensure that systems are properly configured to protect confidentiality, integrity and availability.

1202. Within the Defence environment, any system used to store, process or forward official information may be subject to compliance activity by the appropriate Security staffs, or other competent bodies acting on their instructions, with or without the knowledge of its users.

1203. Compliance activities may be categorised as review, monitoring, inspection and oversight. Responsibilities are shared amongst a number of authorities, as summarised in the table below:

Activity	**Responsibility**	**Performed By**
Review	**System Operating Authority (SOA)**	SOA staff
Monitoring	Security staffs	Specialist technical staff
Inspection	Security staffs	Security and/or technical staffs
Oversight	Departmental Security Officer	DSSO

Principle

1204. The accreditation process ensures that a competent authority has reviewed and accepted the risks to the system as installed. The purpose of compliance is to ensure that the risks to a system are being managed effectively, and to provide a documented basis for continuance of accreditation.

Frequency Of Activity

1205. The frequency of compliance activity is based primarily on the criticality level (CL) of a system, which is assigned, following a risk assessment, by the system owner. Criticality levels are described in **Chapter 1 Annex A**. The tables in this Chapter show mandated and/or guideline frequencies for each type of compliance activity, and relate to all IT systems regardless of size or connectivity. Mandated activity is to be implemented not later than 1 July 2002, but may be regarded as guideline prior to that date.

Security Policy Documentation

1206. Details of the assessed criticality level for all new systems are to be included in the security policy documentation, which is described in **Chapter 3**.

Review

1207. Reviews are performed on behalf of the SOA, to ensure that security is being managed correctly. There are two types of review; Security Reviews and Installation Vulnerability Reviews (IVRs). *Review* should not be confused with *inspection* and *audit*, which are compliance-related activities carried out on behalf of the Principal Security Advisor (PSyA) or Defence Security Standards Organisation (DSSO), and the DSO, respectively.

1208. Security Reviews comprise three main elements:

a. Procedural Review; examination of manual logs such as Document Registers and Room Access Registers. System accounting records should be scrutinised for violations or incidents.

b. Hardware Review; validation of hardware inventories and examination of cable infrastructure.

c. Technical Review; verification that the technical measures applied within the Electronic Security Environment (ESE) are appropriate and operating correctly.

1209. The purpose of an Installation Vulnerability Review (IVR) is to review the System Configuration Model (SCM), as described in **Chapter 3**, against known vulnerabilities, and to ensure that appropriate updates and patches are applied in a timely manner, and the SCM updated accordingly. The IVR must include all aspects of a network including operating system, routers, hubs and firewalls.

1210. The vulnerability information for an IVR will come from a number of sources including specialist advice from MOD and other government agencies, and List X contractor support:

a. General alerts (Vulnerability Warning Notices and Vulnerability Rectification Directives), as described in **Chapter 2** and **Chapter 7**, issued direct to Units by the JSyCC or other governmental advisory services;

b. Platform-specific information from vendors and other public domain sources, including Internet sites.

1211. The the following table shows mandated Security Review and IVR activity levels, which should be increased by one level if the system is connected directly or indirectly to the Internet.

System Profile	Security Review	Installation Vulnerability Review (IVR)
CL1	Weekly	Weekly
CL2	Monthly	Monthly
CL3	Quarterly	Quarterly
CL4	10% of systems checked annually	

Monitoring

1212. Monitoring describes non-invasive procedures aimed at enforcing good security practice. Monitoring is performed on behalf of the Security staffs either by the SOA or an external agency.

1213. Monitoring may be categorised as:

a. CompuSec monitoring, which includes the use of Intruder Detection Systems (IDS) or e-mail screening;

b. ComSec monitoring;

c. RadSec monitoring, which consists of :

(i) TEMPEST monitoring;

(ii) ELSec monitoring

(iii) FRSec.

1214. MOD policy on the use of IDS is still developing, but the broad principle is to use a mix of compatible and interoperable IDS products. Further details are given at Chapter 6.

1215. IDS are not mandated but, where implemented, it is strongly recommended that their output is accessible to a MOD Monitoring and Reporting Centre (MRC), as described in **Chapter 11**, in addition to any local monitoring. IDS provided for Criticality Level (CL) 1 and 2 systems must provide such a feed to a MRC, and the MRC must be capable of responding to IDS alerts whenever the system is operational.

1216. ComSec and RadSec monitoring are carried out by specialist staff from other organisations within MOD or Government. Their use is subject to control by PsyAs

or the DSSO, to whom all reports arising are to be sent.

1217. As a guideline, systems should be subject to ComSec and RadSec monitoring on installation, after major changes and at the frequency shown in the following table.

System Profile	**Frequency**	
	Fixed System	**Deployed System**
CL1	2 yearly	Annually
CL2	5 yearly	2 yearly
CL3/4	Not normally required	5 yearly

Inspection

1218. Inspection describes on-site and/or invasive procedures performed by Security staffs as an independent source of assurance for the Risk Owner. Inspections are typically performed before initial accreditation, after major changes, and subsequently at a frequency appropriate to the system.

1219. Inspecting Staff will be designated by Security staffs, and will normally be drawn from specialist security staffs, or staff from other areas of Government, or contract support personnel.

1220. Weaknesses identified will be graded from E (actual breach) to B (minor shortfall), and action taken in accordance with the table at Annex A.

1221. There are seven types of inspection:

a. GSE/LSE Inspection;

b. ESE Inspection;

c. Vulnerability Analysis (VA) ;

d. COMSEC Routine Inspection;

e. TEMPEST Visual Inspection;

f. IDA/CIDA Conformance Review (ICR/CCR) ;

g. RadSec On-Site Test.

1222. **GSE/LSE Inspection.** A GSE/LSE Inspection ascertains whether the personnel, physical and procedural security measures specified in the security documentation have been implemented as required.

1223. It is recommended that each new system undergoes a pre-installation GSE/LSE Inspection, and thereafter the frequency should be aligned with that for routine protective security inspections based on the security categorisation of units, as specified in **Volume 1**. It is acceptable to address GSE/LSE Inspection on a site basis as opposed to a system basis provided that the whole system is ultimately subject to inspection.

1224. **ESE Inspection.** An ESE Inspection is a basic configuration check of ESE measures to establish whether a system has been correctly configured to meet the technical security measures specified in its security policy documentation. A supporting Vulnerability Analysis (VA) will normally be required.

1225. **Vulnerability Analysis (VA).** A VA uses approved vulnerability tools to actively probe an installation or network for exploitable vulnerabilities, and to analyze and map network connections. Any VA tools used are to be cleared with the system administrator and agreed for safe use by the appropriate Security Authority.

1226. VA are categorised into four incremental levels of effort:

a. **VA Level 1 – Primary Investigation.** Identify and validate all system and connected network elements, analyse topology and locate obvious vulnerabilities and/or initial entry points;

b. **VA Level 2 - Vulnerability Sweep.** Exploit vulnerabilities discovered during VA Level 1, gaining basic access to accounts, and attempt to crack passwords;

c. **VA Level 3 - Security Sweep.** Exploit vulnerabilities for greater access, exploit-trusted relationships, exploit new vulnerabilities;

d. **VA Level 4 – Stress Testing**. Test the system to ensure resilience to denial of service (DoS) attacks. VA4 must be authorised by the Security Authority, in consultation with the operational and business sponsors, and will normally only be appropriate for Criticality Level 1 systems.

1227. The mandated ESE Inspection and guideline VA levels are shown in the following table:

System Profile	ESE Inspection Frequency		Supporting VA Required	
	Fixed Site	Deployed	Fixed Site	Deployed
CL1	On each site installation, then 2 yearly, or after major changes.	On each site installation, then yearly or after major changes.	**VA3** on installation then 2 yearly	**VA3** on deployment then annually

CL2	On first and 50% of subsequent site installations, then 3 yearly, or after major changes.	On each site installation, then 2 yearly or after major changes.	**VA2** on installation then 3 yearly	**VA2** on deployment then 2 yearly
CL3	On first and 25% of subsequent site installations, then 5 yearly, or after major changes.	As part of first and 50% of subsequent site installations, then 3 yearly or after major changes.	**VA1** on installation then 5 yearly	**VA2** on deployment then 3 yearly
CL4	On first and 10% of subsequent, site installations, and after major changes.	As part of first and 25% of subsequent site installations, then 5 yearly or after major changes,	**VA1** on installation	**VA1** on deployment then 5 yearly

Note: *System locations used for ITSEC or CC Penetration Tests will not normally require an initial ESE Inspection or VA.*

1228. VA may be performed by MOD infosec staffs, by specialists from Government Agencies or by contractors. Personnel performing VA must have a minimum SC clearance, except for Criticality Level 1 systems where a minimum DV is required. Advice should be sought from the PSyA or DSSO as appropriate.

1229. Copies of VA reports are to be supplied to the JSyCC who are responsible for collation of the vulnerability picture for MOD as a whole.

1230. **COMSEC Routine Inspection.** Routine inspections are required of all sites holding Enhanced Grade or High Grade COMSEC equipment. Each new implementation will require a pre-installation COMSEC Routine Inspection, and thereafter if there has been any change to the COMSEC equipment installation. More detail is provided at **Chapter 23**, and in the appropriate COMSEC publications.

1231. **TEMPEST Visual Inspection.** A TEMPEST Visual Inspection (TVI) is carried out by trained personnel recognised by the Co-ordinating Installation Design Authority (CIDA), to ensure that appropriate TEMPEST installation control procedures have been applied. It is recommended that each new implementation undergoes a pre-installation TVI, and thereafter if there has been any change to the electromagnetic environmental factors for the system.

1232. **IDA/CIDA Conformance Review.** A Conformance Review is carried out by an Installation Design Authority (IDA), CIDA, or by specialist Government Agency or contractor support, to ensure that the TEMPEST installation control procedures are still being complied with. The guideline Conformance Review frequencies are shown in the following table:

System Profile	IDA/CIDA Conformance Review Frequency	
	Fixed Installations	**Deployments**
CL1	Annually	On takeover from TEMPEST Control Officer (TCO), then 6 monthly
CL2	2 yearly	On takeover from TCO, then annually
CL3	3 yearly	On takeover from TCO, then 2 yearly
CL4	5 yearly	On takeover from TCO, then 3 yearly

1233. **RadSec On Site Test** In some cases, the threat to and vulnerabilities of a particular installation will mean that a RadSec On-Site Test is required, to address either TEMPEST or ELSEC issues, as detailed in **Chapter 21**. This test will be carried out by specialist staffs from the CIDA or from other Government Agencies.

Oversight

1234. Details of the extent to which Sectors have met the requirements for both mandated and guideline compliance activities are to be included in their Annual Security Report.

1235. In addition to the routine compliance activities described in this chapter, the Departmental Security Officer retains the right to inspect without warning any CIS installation within the Defence ambit, including industry and agencies.

This page intentionally left blank.

ANNEX A TO CHAPTER 12

GRADINGS OF RECOMMENDATIONS FROM COMPLIANCE ACTIVITIES

1. The following table indicates the actions that are to be taken when weaknesses are identified during compliance activities.

Grade	Meaning	Immediate Action	Remedial Action	Clearance Procedure
E	An actual information security breach has been detected.	1) Cease processing unless operationally/ business critical and physically secure system. 2) Raise Incident Report.	Immediate remedial action is required before processing is resumed.	Approval by relevant PSyA or DSSO before processing is resumed.
D	Security weaknesses which may be exploited to cause a serious breach of information security have been identified	1) Immediate action should be taken to limit any potential damage. 2) Raise Incident Report.	Remedial action is required within 1 month	Approval to both continue processing and for rectification must be sought from the relevant PSyA or DSSO.
C	Security weaknesses which may be exploited to cause a breach of information security have been identified		Remedial action is required within 3 months	
B	An minor shortfall of technical, physical or procedural security has been identified		Remedial action is required within 6 months	
A	*Best Practice* recommendations	No specific requirement		

2. In all cases, remedial action will include :

a. Technical, physical or procedural changes ;

b. Re-verification of conformance to the minimum security standards ;

c. Verification activities as required by the DSSO or PSyA;

d. Any necessary amendment to Security Policy Documentation.

3. In certain specific cases, identified weaknesses should be graded as follows :

Symptom	System Profile	Grade
System not Accredited	TOP SECRET, Compartmented, or CL1	E
	SECRET or CL2	D
	Other	C
System not being operated in accordance with its current Accreditation and/or has severe shortcomings in its Security Documentation	TOP SECRET, Compartmented, or CL1	D
	SECRET or CL2	C
	Other	B

SECURITY IN THE PROJECT LIFECYCLE

This page intentionally left blank.

CHAPTER 13

SECURITY IN THE PROJECT LIFECYCLE

Introduction

1301. This chapter deals with security activities in the system lifecycle for IT systems of a larger and more complex nature. The operation of such systems will, almost certainly, involve specialist staff to manage their technical operation, and it is important to realise that security considerations start very early in the procurement cycle.

1302. It covers both "Vote 1" (non-operational. and "Vote 3" (DPA led) procurement procedures, and by alternative measures such as those installed and operated for MOD by PFI and PPP partners. Systems not procured using these methods are still subject to security input, and all procurement is to follow the guidance given in JSP 343 (MOD IT Project Guide).

Security Considerations At The Planning Stage

1303. The introduction of security features into an existing system/environment can be time-consuming and costly. Much expense, time, and inconvenience will, however, be avoided if the system and installation are designed with security considerations taken into full account from the outset.

1304. This requires the total involvement of the security staff from the initial planning stages, and throughout development and installation, so that maximum benefit can be derived from the recognised authorities in the various fields of computer security. Defence Security Standards Organisation (DSSO) or TLB Principal Security Adviser (PSyA) staff or their nominated representatives are to be informed when proposals are submitted for a new or enhanced installation.

1305. At the outset of a project the nature of the Security Policy Documentation that is required should be agreed with the MOD accreditor. This is particularly important if a contractor is being employed to produce the Security Policy Documentation.

1306. An IT Security Working Group (SWG) must be established for all large, complex or operational CIS systems and projects. The SWG is to be formed from the outset for all CIS systems and projects, and is to be chaired by a senior member of the project/system staff, who will also provide resources, accommodation and administrative support for the SWG. The SWG is responsible for all aspects of security within the project or system and for supporting the accreditor and project sponsor. It reports to the project sponsor, accreditor and project board, and is to meet at frequent intervals, as determined by the project sponsor and accreditor, throughout the whole lifespan of the project or system. The role of the SWG is covered in **Chapter 2**.

Targets Of Accreditation

1307. Defining the scope of a large and distributed IT resources in terms of boundaries and management responsibilities is a complex and on-going task. Particular difficulties arise from:

a. Communication Systems;

b. Systems where individual data elements when aggregated would attract a higher protective marking level;

c. Cases where the scope and function of the system is still evolving or may be planned to have a dynamic architecture.

1308. A different perspective being offered may also mean an end-user service formed from a number of "layers", each of which may have its own security requirements, and care must be taken to ensure that layers are mutually co-operative and do not undermine each others security functionality. A typical example of a layered approach would be:

a. Bearers;

b. Infrastructure (client and server computers and their operating systems);

c. Services / Applications.

1309. It is worth noting the way in which this security "layering" differs from that used in ISO7498 (the Open Systems Interconnection (OSI) Reference Model (RM)) and the Internet Protocol (IP) suite, which are both also layered approaches, can be seen from the diagram below:

OSIRM		**IP Layer**	**Security Layer**
Level	**Function**		
7	Application	Application	Application
6	Presentation		
5	Session		
4	Transport	Transport	Infrastructure
3	Network	Network	
2	Data Link	Link	Bearers
1	Physical		

1310. The Target of Accreditation, once agreed, may become contractually binding where the implementation of a CIS is to be carried out by a contractor. In such cases, changing MOD requirements after contract let will not normally be applied retrospectively without agreement by both the Accreditor and Project Management Authority.

Domain Based Approach

1311. A framework for the management of security within MOD is being developed, based on the domain-based approach to Accreditation, with the aim of minimizing risk in complex projects and will be incorporated into future issues of JSP440 Volume 3. The framework describes a MOD accreditation cycle which divides security activities, including risk assessment and risk management, into four phases: scoping the security problem; appraisal of the security options; provision of an accredited system and maintenance of the security of the system in service.

1312. Projects interested in the use of the Domain approach should consult EC(CCII)IOCMProj via their PSyA for further information and advice as to the applicability of the technique to their needs.

Security Activities

1313. CESG Computer Security Memorandum No 11 (CM11), "Security Activities in the Project Life-cycle", identifies the major security activities that are to be undertaken during any Project, from the Project Identification stage to the Contracts. Responsibilities relating to the significant security activities in an IT system from conception, feasibility studies, through to the issue of contracts are also addressed.

1314. The responsibilities relating to the significant security activities in an IT system from conception, through feasibility studies, and to the issue of contract are also described in this section. The potential attractiveness of systems that can store or process protectively marked data, or data with special caveats, will in most cases necessitate evaluation and certification.

1315. It is strongly recommended when initiating a new project that Project Names are drawn from Codeword index to prevent duplication.

Extramural Assistance

1316. For large and complex systems, it is likely that in addition to the security resources available from with the Project Management or System Operating Authorities respective organisations, additional specialist assistance will also be needed.

1317. The following table uses the Risk Categories laid down at **Annex A to Chapter 14** to determine the requirements for extramural assistance:

<table>
<tr><th>Risk Category</th><th>SAC</th><th>EC(CCII)IO CMProj</th><th>NTA</th><th>DSSO</th></tr>
<tr><td>A</td><td rowspan="3">Mandatory</td><td rowspan="3">Mandatory</td><td rowspan="2">Mandatory</td><td>Mandatory</td></tr>
<tr><td>B</td><td rowspan="2">Recommended</td></tr>
<tr><td>C</td><td>Recommended</td><td rowspan="3">Not required</td></tr>
<tr><td>D</td><td>Recommended</td><td rowspan="2">Not required</td><td rowspan="2">Not required</td></tr>
<tr><td>E</td><td>Not required</td></tr>
</table>

1318. Details of the categories of assistance are as follows:

a. SAC (Security Assurance Coordinator) – specialist advisor, normally contractor support, as laid down in Chapter 2 ;

b. EC(CCII) – the staff of EC(CCII)IOCMProj provide a MOD Infosec Coherence function, and should be consulted where technically complex solutions are required ;

c. NTA (National Technical Authority) – the consultancy group within the Communications-Electronic Security Group at Cheltenham should be consulted where technically demanding solutions are required ;

d. DSSO (Defence Security Standards Organisation) – where the requirement suggests any solution would involve a departure from established MOD security policy, DDefSy must be consulted.

Resource Implications

1319. When initiating a Project, it is important that the resources required for security throughout the lifecycle are identified at an early stage, both in terms of personnel and budget. The following table identifies the main security costs likely to be encountered during a system lifecycle:

Phase	Activity	Resource Type(s)
Inception	Security Assurance Co-ordinator (SAC)	Staffing
	Specialist consultancy support (e.g. CESG)	Funding
Development	Security Assurance Co-ordinator (SAC)	Staffing
	Specialist consultancy support (e.g. CESG)	Funding
	COMSEC hardware	Funding
	COTS / GOTS Infosec software	Funding
	Evaluation and Certification	Funding
	Works services	Funding
Operation	Security Assurance Co-ordinator (if still evolving)	Staffing
	Specialist consultancy support (if still evolving)	Funding
	System Security staff (possibly multiple sites)	Staffing
	COMSEC material (e.g. KVs)	Funding
	Security consumables (e.g. badges, seals, CD-R)	Funding
	Security management software (e.g. IDS)	Funding
	Security infrastructure (e.g. MRC communications)	Funding
	Compliance Checks	Funding
	Non-functional equipment / media disposal	Funding
Withdrawal	Equipment / media disposal	Funding

1320. This table is by no means an exhaustive list of the activities that may require project resources, and PSyA advice should be sought before finalising this list for a project.

Vote 1 Procurement

1321. The PRINCE Project Management methodology, which is mandated for Defence non-operational systems over a specific value, does not specifically cover IT Security. It is the Project Manager's responsibility, however, to ensure that the system implemented meets security requirements.

1322. For large and complex projects and systems, or sites/formations with extensive use of IT systems, a Security Assurance Coordinator (SAC) should be appointed, both to provide advice and assistance to the project / system management authorities, and to reduce the resourcing implications being placed on external agencies such as Accreditors.

1323. The role of a SAC is one of the "permitted extensions" to the functions of a Project Assurance Team (PAT) as laid down within the Governmental PRINCE methodology, and can also be considered to be an expansion upon the role of an IT Security Officer (ITSO). Details of the Terms of Reference (TOR) for a SAC are laid down at **Chapter 2 Annex D**.

Vote 3 Procurement

1324. The procurement of "Operational" systems in MOD is accomplished under Defence Vote 3 by following a set of prescribed procedures known as the DPA route. This section identifies the major security activities that are to be undertaken during the procurement stages of this route from the Concept Formulation and Preliminary Study stage to the Full Development stage.

1325. The Smart Procurement Initiative has led to a more tightly coupled acquisition approach based upon joint MOD and Industry manned Integrated Project Teams (IPTs).

1326. The full repercussions of these changes have not been finalised as yet, advice as to the best practice for this new system should be sought from the PSyA, who will hold the Interim Guidance Note (IGN) and Defence Information Assurance Notice on this subject.

1327. The Security Policy Document structure is described in **Chapter 3** and it fulfils the requirements of the Accreditation Document Set (ADS) described in HMG Infosec Standard No 2. Several of the documents specified in Chapter 3 derive from the work on domain based accreditation.

1328. The accreditor's agreement would generally coincide with project milestones, such as Initial Gate, Main Gate (under Smart Procurement), development contracts or

user trials. The accreditor can agree the required Accreditation Evidence Statement and project risk related documents as an Infosec Management Plan (IMP), in the early stages of the project (probably around Initial Gate). The IMP applies to the project, and is concerned with their management of the accreditation process for one or more Targets of Accreditation.

1329. The minimum security contribution to Initial Gate is an Infosec Scoping Appraisal (ISA). Agreement of the ISA is the accreditor's way of indicating that he/she is happy that the need for security and accreditation have been adequately recognised by the project. The ISA should be short, no more than 6 pages, and maybe only a single side. It should contain the security scope of the project, links and dependencies, the key factors influencing the Operational Security Management Plan, and an outline IMP. The level of security-related project risk is given by a Security Risk Category, which determines whether or not a Security Working Group and/or detailed IMP are required.

1330. For complex projects the accreditor may endorse an Infosec Risk Management Appraisal before Main Gate. This records the results of the project's appraisal of solution options and justifies which they will develop into a Target of Accreditation and accompanying ADS. In simpler projects, the accreditor may be able to endorse either or both the Security Risk Assessment and Security Requirements Statement before Main Gate.

Evaluation And Certification

1331. Accreditation may need to be supported by certification in accordance with minimum standards. Systems, which require certification by the Certification Body, are to be evaluated by a licensed Evaluation Facility. Evaluation and Certification are covered in greater detail in **Chapter 6**.

Business Continuity

1332. Disruption can arise due to the failure of system components, denial of access or corruption of stored information. Unless planned for, retrieval of data after a disruption is often difficult, time-consuming and sometimes impossible.

1333. Business Continuity addresses what needs to be done to ensure that key activities can survive disruptive events. It involves the identification of priorities and the application of risk management to what has traditionally been termed disaster recovery. Business Continuity embraces more than just IT: it includes people and processes, accommodation, paper and electronic records. More details on Business Continuity are given in **Chapter 1**.

Compliance

1334. The achievement of Accreditation for a system declares that an Accreditor, as a Competent Authority has reviewed and accepted the Risks and their Management for the

system(s) as installed. The validity of this situation can only endure as long as the Risks do not change, and the configuration is unchanged.

1335. To maintain effective security for the lifetime of a system, in addition to the measures inherent in Project Management structures such as Security Working Groups (SWG) and Configuration Management (CM) Boards, additional procedures are required that ensure ongoing compliance with security requirements until the system is finally withdrawn.

1336. Any system used to store, process or forward Official Information may be subject to technical or procedural Compliancy review by appropriate MOD Security Authority staffs, or other Competent Bodies agreeable to MOD Security Authorities.

1337. All Compliancy activities result in some form of deliverable, typically a report, being generated for use by the Accreditor(s) as evidence for continuance of Accreditation. Compliance checking is covered in detail in **Chapter 12**.

System Close Down

1338. The security activities for this stage are to be documented in the Project Plan. The removal of all information, both in electronic form and hardcopy, which has been stored or processed by the system are to be in accordance with the specified security procedures. Prior to the system's removal from service, information about the organization of the configuration is to be retained for traceability purposes.

1339. There may be systems, the nature of whose configurations is sensitive, where the close down stage is to comply strictly with specified security measures and be in accordance with prescribed guidance on computer security requirements and the security regulations described elsewhere in this volume.

1340. Disposal of surplus CIS equipment and media that has held or processed protectively marked material is covered in **Chapters 4 and 5**.

This page intentionally left blank.

RISK ASSESSMENT AND RISK MANAGEMENT

This page intentionally left blank.

CHAPTER 14

RISK ASSESMENT AND RISK MANAGEMENT

Introduction

1401. This chapter provides generic guidance on Risk Assessment and Risk Management and does not specify a methodology to undertake the analysis and management activities required. Risk Assessment and Risk Management are treated as two related but separate activities. Risk Analysis is the identification and assessment of the risks, based on asset values, threats and vulnerabilities. Risk Management is the process of identifying, controlling and minimising or eliminating security risks to an acceptable level and involves managing the uncertainty within the risk analysis itself

1402. Information Assurance is fundamental to MOD's business. The effective conduct of MOD operations requires that the security (which includes confidentiality, integrity and availability concerns) of information and services are not subjected to unacceptable risk of compromise.

1403. A framework for the management of security within MOD is being developed, based on the domain-based approach to Accreditation, with the aim of minimizing risk in complex projects and will be incorporated into future issues of JSP440 Volume 3.

1404. The framework describes a MOD accreditation cycle which divides security activities, including risk assessment and risk management, into four phases:

a. Scoping the security problem;

b. Appraisal of the security options;

c. Provision of an accredited system

d. Maintenance of the security of the system in service.

Methods

1405. Formal Risk Analysis and Management methods are now necessary to cope with the complex security problems presented by information systems and networks.

1406. The following are examples of some the Risk Analysis and Management methods:

a. Supplement 2 to the Manual for Protective Security, provides an outline Risk Management method This includes a matrix for calculating risk together with an eight step management cycle*;*

b. CRAMM Version 3 is the UK Government's Risk Analysis and Management Method for IT systems. CRAMM follows a three staged approach and is supported by a software tool;

c. The Guidelines for the Management of IT Security (GMITS) is an internationally recognised ISO/IEC management guideline for IT security;

d. The Guide to BS 7799 Risk Assessment and Risk Management addresses the subject in the context of BS 7799;

e. There are also several proprietary methods available, supported by automated tools, for assessing risks.

1407. It is for the project manager to decide the most appropriate method to be used, in conjunction with the Accreditor. In some cases it is not necessary to carry out a full risk assessment for every project since many systems will operate within the boundaries of higher level MOD security policy. The Accreditor will confirm whether an existing risk assessment is both current and comprehensive enough for the purpose in hand. In a full risk assessment all assets will be identified together with the asset owners who may be accountable for whether the risks to a particular asset justify particular levels of investment in counter-measures.

Risk Analysis

1408. Risk is dependent on the asset values, the threats, and the vulnerabilities. Risk Analysis involves the identification and assessment of the levels of risks calculated from the assessed values of assets and the assessed levels of potential threats to, and the potential vulnerabilities of, those assets. The range of risks to IT systems is complex and requires proper analysis to ensure that the risks are adequately managed. Like all business risks, the level of risk changes with circumstances.

1409. The risks to MOD IT systems that may affect the confidentiality, integrity, availability and the legal and regulatory compliance of IT resources must be identified. Risk may be present where a potential threat coincides with a potential vulnerability. Effective assessment of risk will require the assistance of both business managers and IT systems staff, possibly using other experts as required on technical issues.

1410. HMG Infosec Standard No.1 (HMG IS1) is the Government standard for assessing technical risks i.e., those that affect the design and configuration of an IT system. HMG IS1 provides guidance about how strong electronic counter-measures should be in particular circumstances. HMG IS1 is mandatory for all HMG IT systems carrying protectively marked information. The results of this method are key to the IT Security Evaluation and Certification Scheme and the Common Criteria, for the evaluation of the strength of security features. The MOD interpretation of HMG IS1, together with additional guidance, is at **Annex B to Chapter 6**.

Risk Assessment Activities

1411. The Scoping phase of the Accreditation cycle requires the production of an Infosec Scoping Appraisal (ISA). An HMG IS1 or detailed risk assessment does not need to be conducted for an ISA. Instead, a simplified risk assessment should identify the level of risk to the project arising from the need for security controls and accreditation. The risk should be assigned a Security Risk Category on a scale of A-E, where A represents a very high risk to the project and E a very low risk. Security Risk Categories are fully defined in **Annex A**.

1412. The Appraisal phase for all but the simplest projects requires the comparison of options based on an assessment of security risks, the results of which are recorded in an Infosec Risk Management Appraisal (IRMA). An HMG IS1 risk assessment is required for each of the options discussed in an IRMA, but the assessment need not be detailed.

1413. During the Provision phase, accreditation evidence is compiled, including a full Security Risk Assessment (SRA). Risk analysis for a SRA involves full assessment of the assets to be protected, the potential threats and vulnerabilities, including IS1 calculations, combined with the strength, effectiveness and assurance levels of the protective measures to be provided both by the project and by other means.

1414. During the Maintenance phase, further risk assessment is required when there is a significant change to the perceived threats, the system itself, or its mode of use. This re-assessment updates the Security Risk Assessment.

Asset Identification and Valuation

1415. The boundary, for the system(s) that forms the Target of Accreditation, should be carefully established before identifying assets. All sensitive and valuable assets within the boundary, which are essential to the business process, should be identified.

1416. Assets are divided into groups typically as follows:

a. Information and data assets;

b. Software assets;

c. Communications;

d. Physical assets;

e. People;

f. Services;

g. Utilities.

1417. Values, which represent the importance of the assets to the business, should be assigned to each asset. These can be expressed in terms of confidentiality, availability and integrity, and an asset could therefore have its value expressed at three different levels.

Asset Register

1418. An asset register is not an inventory or configuration control record book. The granularity should be set by the range of values and asset owners rather that numbers of items, processes etc. At its most complex it might embrace a complete register of all the various CIS assets. Accreditations involving complex risk assessments and asset valuations will require a full asset register.

1419. Some assets retain the same value to the organisation throughout their operational life. Some change on a predictable basis, and some unpredictably. If these variations in asset value are likely to occur, the details should be recorded in the asset register. This will ensure that risk management decisions reflecting value variations are clearly linked to an organisation's business processes.

Threat Assessment

1420. For each asset or asset group a list of both the types, including environmental if applicable, and levels of threat should be drawn up. It is necessary to assess the likelihood of a threat being enacted and this should take account of:

a. Threat frequency;

b. Deliberate;

c. Accidental.

Vulnerability Assessment

1421. The vulnerabilities of each asset or groups of assets should be identified and an assessment made of the levels of those vulnerabilities. The level is an indicator of how serious each vulnerability is and the likelihood that if a threat was to manifest itself that the vulnerability would be successfully exploited. The vulnerability level should also reflect the probability that vulnerabilities will be discovered in the system during its lifetime.

Risk Management

1422. Risk Management is the process by which perceived risks are eliminated, reduced, accepted or transferred. This involves the identification, selection and adoption of countermeasures to the identified security risks, to reduce them to a level that is assessed as acceptable. It may also involve activities to manage the uncertainty of a risk assessment through monitoring or risk reduction studies, planning for repeat assessments and preparing contingency plans should the risk prove unacceptable in the future. A balance has to be agreed between proactive and reactive risk management measures.

1423. Risk Management responsibilities, and ownership of risk, must be clearly identified, agreed and assigned. Accountability can be achieved by the use of a Risk Management Statement. This is the formal acceptance of which risks are going to be avoided, accepted, transferred or limited, together with acceptance of the costs implied by those choices. The Risk Management Statement will also record any waivers from higher-level risk management decisions.

1424. The following documents, which underpin Risk Management decisions during the ongoing Risk Management process are detailed in **Chapter 3**:

a. Infosec Scoping Appraisal (ISA);

b. Infosec Management Plan;

c. Infosec Risk Management Appraisal (IRMA);

d. Security Risk Assessment (SRA).

Accreditation

1425. The goal of the Accreditation process will be to gather evidence that residual risks have be minimised to an acceptable level. Evidence of this for most non-technical facets of security will be demonstration of compliance with MOD baseline security standards. For the 3 technical aspects, as well as compliance with baseline security standards, the organisation(s) responsible for the system's implementation should demonstrate that no unacceptable risk from actual or potential significant exploitable vulnerabilities, or risks of failure of security functionality, exist.

1426. Accreditation does not obviate the need for a subsequent management approval process whereby the System Operating Authority(s) (SOA) and Data Owner(s) accept any residual risks identified by the accreditation process.

Compliancy

1427. The achievement of Accreditation for a system declares that an Accreditor has reviewed and accepted the Risks and their Management for the system as installed. The validity of this situation can only endure as long as the Risks do not change, and the configuration and mode of use is unchanged.

1428. To maintain effective security for the lifetime of a system, in addition to the measures inherent in Project Management structures, additional procedures are required that ensure ongoing compliance with security requirements until the system is finally withdrawn. These are detailed in **Chapter 12**.

ANNEX A TO

CHAPTER 14

SECURITY RISK CATEGORIES

1. Five Security Risk Categories, A-E, are defined. The categories broadly group projects according to the degree of security risk to information inherent in the requirements. The assumption is that a greater security risk gives rise to security requirements that may be difficult to implement and that this increases the risk to the project. The Security Risk Categories are:

Security Risk Category	Likely level of risk to the Project arising from the security requirements
A	Very High Risk
B	High Risk
C	Significant Risk
D	Low Risk
E	Very Low Risk

2. For each category the key mechanisms by which the accreditor and project team should communicate to manage a successful accreditation process are defined. The risk management strategies for the categories are distinguished according to the requirement for a Security Working Group (SWG) and the formal endorsement of the Infosec Management Plan (IMP) by the accreditor(s).

Security Risk Category	Accreditor endorsement required		Security Working Group required
	Infosec Scoping Appraisal	Infosec Management Plan	
A	The accreditor(s) or D Def Sy must be consulted before the project can proceed further.		
B	Yes	Yes	Yes. Advice from technical security experts will be required.
C	Yes	Yes	Yes
D	Yes	Yes	No
E	Yes	No	No

3. The policy on the choice of Security Risk Category, Appendix 1, is largely concerned with the Protective Markings, Criticality Levels and clearances associated with the business to be supported by the Target of Accreditation, the anticipated infrastructure and the expected connections. Projects where there is a wide disparity between maximum Protective Marking and minimum clearance will tend towards a high Security Risk Category. Guidance on how to apply the policy as part of an Infosec Scoping Appraisal is provided in the Defence Information Assurance Notice (DIAN) on Security Policy Documentation.

APPENDIX 1 TO

ANNEX A TO

CHAPTER 14

SECURITY RISK CATEGORISATION POLICY

Introduction

1. The basis of the security characteristics of the total system of systems in which the products of the project will reside. The policy is stated in terms of the areas of the business and the parts of the planned or existing infrastructure that can be clearly separated from each other.

2. The Security Risk Category for a project shall be no lower than any of the values determined from the table on page 3 for every area of business or infrastructure that is within the scope of the project, or that will involve assets that the project is responsible for or directly uses. Areas of business or infrastructure may be grouped together to ease the analysis.

3. Wherever there is any uncertainty in determining some factor, a worst case shall be assumed. The accreditor(s) shall always endorse the choice of Security Risk Category, usually through an Infosec Scoping Appraisal (ISA). Any queries or problems with interpreting this policy should be directed to the project's accreditor(s) or to D Def Sy.

Concepts

4. Areas of business are referred to as 'business domains' and parts of the infrastructure as 'infrastructure islands'. If the operational requirements do not allow the information exchange requirements to be predefined and constrained, all of the data and all of the people that the procurement will support, including those they interact with in other systems, shall be considered as a single business domain. Similarly, if the components that implement data exchanges between different parts of the infrastructure cannot be identified, isolated and managed, all of the infrastructure supporting or connected to the system to be procured shall be considered as a single infrastructure island.

5. Where separate business domains or infrastructure islands can be identified, these shall be 'directly connected' and 'indirectly connected' under the following circumstances:

a. Two business domains shall be directly connected if there is a requirement for data to be exchanged, in both or just one direction, in the conduct of that business;

b. Two infrastructure islands shall be directly connected if it is technically possible for data to be exchanged, in both or just one direction, independently of whether or not the business under consideration requires such an exchange to take place;

c. Two business domains that are not directly connected shall be indirectly connected if any business path exists between them, not just if they both do business with a common third party;

d. Two infrastructure islands that are not directly connected shall be indirectly connected if it is technically possible for data to be exchanged under some circumstances.

6. A business domain or infrastructure island is referred to as 'internal' if at least some part of it is within the scope of the project, or will involve assets that the project is responsible for or directly uses. Any other business domains or infrastructure islands are referred to as 'external'.

Determination of a Security Risk Category

7. All internal business domains and infrastructure islands shall be used to determine the Security Risk Category for a project. For each, the table on page 3 specifies minimum requirements and the special cases that require a higher category (with A being the highest). These cases include the required connections to external business domains and infrastructure islands. The Security Risk Category shall be no lower than all the values derived from the table on page 3, and may be higher if other security concerns, such as security management or possible technological constraints, are considered to present a higher risk to the project.

8. No one method for determining a Security Risk Category is mandated.

TABLE FOR: **DETERMINATION OF A SECURITY RISK CATEGORY** The Security Risk Category shall be no lower than the minimum requirements and all the special cases that apply. A dash ('-') indicates that a particular case does not raise the category above the minimum requirements.		**MINIMUM REQUIREMENTS**	**SPECIAL CASES**															
			Within the Internal Business Domain				**Within the Internal Infrastructure Island**				**Direct Connections**						**Indirect Connections**	
			Use Group 1 – see below				*Use Group 2 – see below*				*Use Group 1 for connected business domain Use Group 2 for connected infrastructure island*							
			Uncleared	Basic Check	Security Check	Not Authorised	Uncleared	Basic Check	Security Check	Not Authorised	Uncleared		Basic Check		Security Check	Not Authorised	Uncleared	Basic Check
Maximum Protective Marking handled by an Internal Business Domain or Infrastructure Island	Top Secret	C / D [1]	A	A	A	A	A	A	A	A	A / B [2]		A / B [2]		B	-	B	B
	Secret	D	A	B	-	B	A	B	-	B	B		C		-	C	B	-
	Confidential	D	A	-	-	B	B	-	-	B	B		-		-	C	-	-
	Restricted	E	D	-	-	D	D	-	-	D	D		-		-	D	D	-
Maximum Criticality Level of an Internal Business Domain or Infrastructure Island	Criticality Level 1	C	A	A	-		A	A	-		A		A		-		B	B
	Criticality Level 2	C	A	-	-		A	-	-		B		-		-		B	-
	Criticality Level 3	D																
	Criticality Level 4	E																
If any part of the business or supporting infrastructure is intended to be deployable		C																

Notes:

Note 1: The minimum category may only be D if there are no connections.

Note 2: The minimum category may be B if data can only ever be received from the connected business or infrastructure, and can never be supplied by the Top Secret business or infrastructure.

Explanation of Groups

Group 1 is all the people who conduct the business of a domain. The minimum clearance of these people is required.
Group 2 is all the people who have legitimate access to, or are served by, an infrastructure island. The minimum clearance is required.
In addition, the 'Not Authorised' column applies whenever there are people who are not authorised to access all the relevant caveats or codewords that are present.

Further action required: If any 'external' business or infrastructure has a higher Protective Marking than any of the internal ones, the values from the table for the direct and indirect connections from these shall also be identified. If any of these values are higher than the Security Risk Category for the project, this shall be brought to the attention of the project's accreditor so that any necessary dialogue with other accreditors can be initiated.

SECURITY OF INTERCONNECTED CIS

This page intentionally left blank.

CHAPTER 15

SECURITY OF INTERCONNECTED CIS

Scope

1501. The previous chapters have mainly dealt with CIS, whether small or large, that are within the control of a single System Operating Authority (SOA) and have no internal management boundaries.

1502. This chapter considers the interconnection of two or more systems, either within the remit of a single SOA where internal management boundaries are present (e.g. 2 networks of differing protective marking levels) , or crossing SOA boundaries.

1503. The purpose of this chapter is to give general guidance on secure system interconnection, highlight some of the issues, and set out Defence policy for identifying and countering the risks involved.

1504. It is first necessary define some terminology to help align context :

a. **Domain** - used here in the sense as defined in MOD's Domain Based Approach (DBA) to security, being a logical grouping where people work inside a commonly managed computer system ;

b. **Connection** – used here in the sense defined in DBA, being a permitted interaction between people in different domains ;

c. **Intranet** – one or more domains belonging to people within the same organisation, with connections to a commonly managed, shared, infrastructure;

d. **Extranet** – an intranet with connections to additional domains to external organisations ;

e. **Internet** – the world wide collection of interconnected networks.

Security Principles

1505. When CIS interact, it is necessary to ensure that one system does not undermine the protective measures of the other.

1506. The underlying security principles are the standard Confidentiality, Integrity and Availability (CIA), and in this context all data transported from one system to another should be protected from, among others:

a. Unauthorised disclosure ;

b. Unauthorised modification ;

c. Misdirection ;

d. Monitoring ;

e. Replay ;

f. Deletion ;

g. Insertion ;

h. Masquerading ;

i. Repudiation of receipt or origin ;

j. Out of Sequence delivery ;

k. Technical failure of network components.

1507. In order to provide such protection, the philosophy of **Self Protection** is to be applied to all MOD domains. All connections that are made between domains, to intranets, to extranets, or to the internet, must be through a Secure Managed Interface (SMI), which should be implemented under the control of the System Operating Authority (SOA) of the domain(s) being protected. The main purpose of this chapter is to outline security requirements for such SMIs.

1508. Examples of an SMI will range from an internal software port control on a small system connected to Publicly Accessible Network (PAN), through COTS "screening routers" at internal domain boundaries and specialised devices at external domain boundaries.

1509. To aid the protection of interconnected systems, it is vital that the principle of **Least Capability** is strictly adhered to, and that only those communications protocols (including related ports, services and daemons as applicable) required to implement the agreed Information Exchange Requirements (IER) are enabled, with all others being specifically disabled or removed wherever technically possible.

1510. Legacy systems use a variety of underlying communications protocols, the major examples being serial line, XBM/SDLC and X.25/HDLC. The majority of recent and new system interconnections, however, are based around the Internet Procotol (IP) communications suite, and thus the majority of this Chapter is applicable to IP-based interconnections. Where other protocols are proposed, specific advice

should be sought from the Defence Technical Security Authority, InfoSy(Tech), and the relevant Applied Research Program office, EC(CCII)IOCM/Proj1.

1511. The overall security of any "systems-of-systems" can be compromised by the "weakest link", especially in scenarios where discrete security measures are being provided at different levels of the protocol hierarchy. For instance, if multiple (IP) connection routes exist, an inbound FTP Export request that should be blocked by a Transport Level (Return Address Check) Measure at the "intended" Barrier may still deliberately or accidentally Export the data through an alternate route due to the presence of an unblocked Source (Return) Address deeper within the Datagram envelope, necessitating an additional (Application Level) Barrier if holistic security is to be maintained.

1512. All connections should therefore incorporate appropriate Barrier Functions (BF) to control the nature of interconnection between domains, which will normally be as elements of an SMI, with the BFs implemented within Boundary Protection Devices (BPD) (often colloquially referred to as "Firewalls"), but may also have components in Host systems (both Clients and Servers) within the domain(s). Examples of BPDs include Bastion Hosts and Multi-level Secure (MLS) / Multi Security Level (MSL) devices consisting of several discrete elements, such as man-in-the-loop-sanction Security Release Control Tools (SRCT), one-way regulators, and bi-directional, ruleset driven, "guards".

1513. The major classes of BF are :

Barrier Function	Typical Implementation
Transport level *(e.g. network level packet filtration)*	Basic Packet Filter (PF) BPD, usually a Router with address and port/service controls
Format level *(e.g. protocol form factor analysis)*	Enhanced PF BPD, such as a Router with additional proxy functionality
Content level *(e.g. data analysis)*	Application Proxy BPD, providing complete break of IP between interconnected systems
Interactive level *(e.g. user supplied sanction)*	Typically cryptographic or "trusted path" mechanisms in host(s), linked to proxy in BPD

1514. It will be noted that the sequence of BFs has a symmetry with the IP "stack". For most protocols, the efficacy of the controls is increased by adding together multiple Barrier Functions, and an indicative table of efficacy of mechanism is given below :

Efficacy Required	Barrier Function(s) Required
Baseline Protection (BP)	Transport level
Enhanced Protection (EP)	Transport and Format Levels
High Protection (HP)	Transport, Format and Content Levels
Special Protection (SP)	Transport, Format, Content and Interactive Levels

1515. Not all protocols can be practically controlled at each level, and a summary of the credibility of efficacy claims for BF mechanisms in various IP related protocols is given at **Annex A**. Due to the dynamic nature of both the technologies and their vulnerabilities, before proceeding on this basis the Accreditor(s) should be consulted to ensure that no update by an Interim Guidance Notice (IGN) has occurred.

1516. If the proposed implementation involves the use of "tunnelling" technology across an SMI, then both InfoSy(Tech) and EC(CCII)IOCM/Proj1 should be consulted, as such techniques will normally bypass any BFs in place.

1517. The use of the DBA notation, as summarised at **Annex B**, will aid in the assessment of the placement of BF mechanisms.

1518. The use of Real Time Monitoring (RTM) techniques and Intruder Detection Systems (IDS) can provide additional countermeasures where so required. Further details of RTM / IDS are given at **Chapter 12**.

Interconnection Types

1519. Before examining the proposed technical interconnection, the "business" nature of the interaction as predicated by the system's Information Exchange Requirements (IER) should be characterised in terms of the NATO Interoperability Planning Document WP 71-76 of Feb 93, which identifies 6 levels of interconnection. They are reproduced in full at Annex A to this chapter and identify appropriate security measures, and are to be consulted whenever systems interconnect.

1520. Having described the high level nature of the interconnection(s) envisaged, a number of different scenarios for interconnection exist, which can be summarised as :

a. Interconnection between 2 or more CIS of differing security profiles (e.g. of differing protective marking levels) within the control of single System Operating Authority (SOA) via a dedicated infrastructure ;

b. Interconnection between 2 or more CIS of differing security profiles (e.g. of differing protective marking levels) within the control of single System Operating Authority (SOA) via a shared infrastructure ;

c. Interconnection between 2 or more CIS of similar security profiles (e.g. compatible protective marking levels) within the control of differing SOAs via a dedicated infrastructure ;

d. Interconnection between 2 or more CIS of similar security profiles (e.g. compatible protective marking levels) within the control of differing SOAs via a shared infrastructure ;

e. Interconnection between 2 or more CIS of differing security profiles (e.g. of differing protective marking levels) within the control of differing SOAs via a dedicated infrastructure ;

f. Interconnection between 2 or more CIS of differing security profiles (e.g. of differing protective marking levels) within the control of differing SOAs via a shared infrastructure.

1521. It is important that the Risk Analysis is initiated with a firm understanding of which of these scenarios is proposed, as they will influence both the Threat and Vulnerabilities.

1522. The majority of connections currently being requested are based upon the Internet Protocol (IP), which in itself, unlike previous network level packet switching protocols used in Government such as the International Telecommunications Union (ITU-T) X.25, is a connectionless rather than connection-orientated protocol, although some of the higher level protocols it carries (e.g. Transmission Control Protocol – RFC0793) can provide a connection-orientated reliable service.

1523. The IP protocol suite, as detailed in the series of Internet Engineering Task Force (IETF) documents called Request For Comments (RFC), does not directly map to the terminology of the International Standards Organisation (ISO) Open System Interconnection Reference Model (OSIRM) as laid down in ISO7498, but IP (RFC0791) can be considered to approximate to a Network (OSIRM Level 3) Protocol, with TCP/IP or UDP (User Datagram Protocol – RFC0768) approximating to Transport (OSIRM Level 4).

1524. Also as part of the Risk Analysis, it is import to consider in detail the proposed nature of the communications channel itself in terms of NATO Interoperability Planning Document (NIPD) levels of interconnection as laid down at **Annex C**. This will impact upon the way in which any BPDs behave, and thus will impact on the "facilities available" in terms of the Assurance Requirements for CIS as laid down at **Chapter 6 Annex B** :

NIPD Level	Channel Type	Facilities Available
5B	Internet Protocol suite	Extensive
	Other Channels	Normal
	Packet encrypted or "tunnelled"	Very Limited
	Stream encrypted or "tunnelled"	N/A
5A	Internet Protocol suite	Extensive
	Other Channels	Limited
	Packet encrypted or "tunnelled"	Very Limited
	Stream encrypted or "tunnelled"	N/A
4	Internet Protocol suite	Extensive
	Other Channels	Very Limited
≤3	Manual interfaces and "air gaps"	Very Limited

1525. Additionally, where Virtual Private Networking (VPN) technology is used, it may not be apparent whether or not such direct or indirect connection to shared networks exists.

1526. Client-Server VPN (CSVPN), which use encrypted tunnelling either between hosts or between clients and hosts, with encryption under the control of System Operating Authority (SOA), are analogous to Link Encryption and can be considered to provide link level protection commensurate with the Grade of cryptography available, and thus provides separation from shared networks.

1527. On the other hand, Service Provider Furnished VPN (SPFVPN) can be implemented by either Cryptographic or Closed User Group (CUG) mechanisms, outside the control of the SOA, and as such can only be considered to provide isolation from shared networks if both the specific architecture can support this concept, and an appropriate level of trust can be demonstrated in the Service Provider.

1528. Where cryptographic protocols are intended to cross SMIs, specific approval should be sought in advance from the Accreditor(s) as use of cryptography will typically invalidate the BFs within the BPD or SMI.

1529. The SMI must be capable of being constrained to a NIPD Level of interaction appropriate for the Security Profile of the connecting systems, with the maximum permitted information flow characteristics derived from **Annex A**.

Threats

1530. As an extension to the threats to individual CIS, threats to the information being exchanged can arise from:

a. Disaffected authorised users of both the systems exchanging information and systems transporting the information ;

b. Unauthorised users of the systems exchanging information and systems transporting the information ;

c. Agencies external to the systems exchanging information and systems transporting the information ;

d. The malfunctioning of the systems exchanging information.

Vulnerabilities

1531. When considering vulnerabilities, in addition to reviewing the individual CIS components, the following additional factors should be noted :

a. The number of authorised users of the interconnected systems is higher than a single system alone ;

b. Security policies and measures for the interconnected systems may not be identical ;

c. The data passed between the systems may hide malicious software or may have its confidentiality, integrity or availability compromised in transit ;

d. One system may compromise the confidentiality, integrity or availability of other systems to which it is connected.

Sources Of Compromise

1532. From the consideration of Threats and Vulnerabilities, the following specific sources of potential compromise to interconnected CIS can be summarised :

Confidentiality	Integrity	Availability
Accidental Leakage	Corruption of information (Malicious Code)	Denial of Service (Malicious Code)
Deliberate Leakage	Spoofing (masquerade)	Denial of Service (Flooding)
Stimulated Leakage (masquerade)		
Stimulated Leakage (Trojan Horse)		

Specific Security Measures

1533. Within Defence the following specific interconnection risks will be assessed and policies followed so that:

a. Security is not endangered by the interconnection of specific CIS ;

b. The integration of Defence CIS, in general, can take place in an orderly fashion.

1534. Measures to implement these policies will vary between systems and change as technical progress is made.

1535. **Service Minimisation**. The Least Capability principle is to be applied to the services offered to users and to less protected domains, with the services being kept to the minimum necessary to support the required business activities.

1536. **Import Restrictions**. Information objects imported by a system are to be subject to inspection and only accepted if a sufficient degree of assurance exists that it is safe to introduce them.

1537. **Technical Resilience**. System services are to be implemented in such a way that the security impact of a technical failure is acceptable and proportionate to the perceived chance of failure, whether that failure is deliberately induced or accidental.

1538. **Proactive Management**. Systems and security management must have the resources and skills to detect and deter attacks, and to manage the response adequately, with minimum disruption to the business. All staff, including Accreditors, must be flexible to learn from any incidents and to apply the results quickly and effectively.

Interconnection Scenarios

1539. All such connections require a formally constituted SMI, which will consist of one or more BPD, and any necessary BF within Hosts. Any SMI which consists of multiple components will normally have a differing degree of assurance in their strength.

1540. As a general principle, the components with the highest degree of assurance should be those "facing outwards", a configuration colloquially referred to as presenting a "hardened" edge device to the main attack vector. For example, if 2 BPDs are used to control a TCP/IP based connection, the one with the highest assurance level, or the one with the greatest percentage of its networking software within the Certified baseline, should be used as the hardened edge.

1541. **Connections to non-MOD infrastructures** Where Extranet connections are to be made, or connections to non-MOD Domains or Intranets are required, their technical security measures must be assumed to be inadequate, along with the controls exercised over their users. No recognition of the efficacy of SMIs provided by the non-MOD end of an SMI is to be assumed. The following specific constraints should be applied to the MOD controlled SMI, which must be under the direct control of the MOD SOA.

1542. A detailed methodology for analysing such connections is given at **Annex D**. For most instances, the SMI must be capable of being constrained to a NIPD Level 4 degree of interaction, as laid down at **Annex C**, which will therefore normally be limited to one of the following information flow characteristics:

a) Uni-directional or Bi-directional Messaging across the SMI ;

b) "Export" or "Publication" across the SMI ;

c) Retrieval of information from either the external system(s) or a shared

Export Repository (normally within the DMZ) across the SMI (for instance from Web sites, databases and directories).

1543. Countermeasures against the risks will need to be provided either within a Boundary Protection Device (BPD), the connected MOD domain(s), or some combination of the two. In particular the function of an Export Sanction is to be incorporated to guard against Accidental Leakage, and limit the attractiveness of Deliberate Leakage across the SMI.

1544. At the simplest this will be a BPD which implements a technical mechanism such as a Discretionary Message Guard ("Mail Guard") or Trusted Publisher, or a manual control such as a Releasing Officer, utilising a Security Release Control Terminal (SRCT).

1545. Although Accreditors may wish to agree specific solutions to meet implementation specific considerations, the following measures within an SMI will normally be required to meet the protocol control requirements laid down above :

a) Provide Access Router and Packet Filter functionality at the external boundary, to which all connections external to the managed domain are to be made. For simplicity and manageability, this function should normally be provided in a discrete BPD. The access router should be configured in accordance with the latest Internet Engineering Task Force (IETF) filter guidance including *RFC1858* and *RFC3128*. In particular, the Network Ingress Filtering guidelines laid down within the latest version of the Internet Engineering Task Force's (IETF) Best Current Practice (BCP) Guide Number 38 (*RFC2827* at time of the publication of this document) should be implemented, and the router should also capable of being dynamically managed to block out any external systems that are found to be flooding the internal domain ;

b) Providing screening Router functionality at the internal boundary, ideally in a separate BPD for simplicity and manageability;

c) Typically be a dual homed Bastion host device, or as a minimum provide Network Address Translation (NAT) ;

d) Provide split DNS to guard against the Port 53/UDP attacks that most commercial FireWalls are vulnerable to ;

e) Provide for both incoming and outgoing address restrictions, at both the transport (IP) and application (e.g. mail address) level. In particular care should be taken to limit the maximum number of email addresses that are accepted from an external domain in any one message to obviate Denial of Service (DoS) risks, with a authorisation procedures to constrain the release of such message only to appropriately designated personnel;

f) Provide support for Export Control :

either

(i) Validation by a Mail Guard (for X.400/SMTP and NNTP), or similar device (for other protocols), of a user-supplied authorisation. This will normally be a digital signature applied by trusted path mechanisms, but a Label Hash or Envelope Label (e.g. STANAG 4406 for X.400 or 'X-Sec-Label:' for SMTP) may be acceptable in low risk environments. The use of a simple textual value (e.g. UNCLASSIFIED) within the envelope "Subject:" field is not permitted for new implementations, as it is neither "sealed" whilst in transit, nor immune from Accidental mis-parsing, as a legitimate Subject may include the same letter combinations. In legacy instances, until export control mechanism can be implemented, where the external domain is an unprotected Public Bearer (e.g. the Internet), the Mail Guard or Releasing Officer should at the very least be capable of reforming the envelope without any eye-readable Protective Marking to remove the inference that the Mail originated from a system holding Protectively Marked material;

or

(ii) Implement a Security Release Control Terminal (SRCT) function to filter all outgoing traffic ;

g) Provide comprehensive accounting records, which must include a copy of message contents if the SMI is acting as an MSL device ;

h) Provide Message Content Analysis Guard (MCAG) functionality, to :

(i) Validate incoming messages for Malicious Code ;

(ii) Constrain Attachments (where allowed) to the permitted types as laid down in the relevant Defence Information Assurance Notice (DIAN) ;

i) Where HTTP browsing to hosts outside the domain is to be provided, include functionality either at the external boundary or the client to validate any HTML or URL that may contain Mobile Code such as ActiveX or Java/JavaScript in line with the advice at **Chapter 6**;

j) Any inward connections for Browsing or File Transfer should be constrained to the Export Repository within the DMZ ;

k) When connecting to a hostile environment such as the Internet, consideration should be given to the creation of a "sacrificial pawn" or "honey

pot" which can be monitored for signs of any attack (there being no legitimate need ever to connect to such any host, any connection attempts can be considered as *prima facie* evidence of any attack, to be handled as laid down in **Chapter 11**).

1546. Security Policy Documentation (SPD) for the interconnection, prepared in accordance with **Chapter 3**, must specifically enumerate the generic requirements from this Chapter, and any additional ones identified for the specific interconnection, and show clear evidence that adequate measures have been taken. This will either be in the form of a Statement of Conformance with the relevant Code of Connection(s) (CoCo), or an Interconnection Security Measures Statement (ISMS).

1547. Where connections are only to be made between domains or to intranets of similar security profiles, BF are still required, but predominantly will be Transport BPD configured to maintain separate managerial control, and to minimise the impact of any technical Denials of Service (DoS) that may occur on connected domains, whether accidental or deliberate.

Risk Assessment

1548. The means of implementation for these policies will depend to a considerable extent on the level of interconnection. For instance,

a. Where systems exchange information by an authorised user copying from one screen to another (i.e. Level 2), personnel, physical and procedural measures may be sufficient ;

b. In other where systems are open to each other electronically (i.e. Level 4,5A or 5B), the appropriate technical measures are derived from the level of interconnection.

1549. The detailed functionality of the SMI will need to be determined on a case by case basis, based upon connection scenario, NIPD level and channel type(s). It is, however, stressed that as a minimum each SOA should have at least one BPD within a SMI which is under their direct management control (e.g. screening router between "internal" LAN and shared LAN / WAN).

1550. Protection for information in transit may be provided completely or in part by the bearer system or by the end systems (i.e. if super-encryption is required). The systems may, or may not, have addressing and security labelling which are intelligible to each other and this could either be applied by an application (e.g. X.400/500) or by the operating system.

1551. Assurance Having established the functionality requirements for SMI / BPD / BF, the methodology laid down at Chapter 6 Annex B for calculating ESE

assurance requirements must be followed.

1552. Technical security measures will normally require a formal ITSEC evaluation, and, if based upon COTS Certified packages, a further Penetration Test to confirm correct configuration.

Accreditation

1553. **Functionality**. Before approving the system interconnections, the accreditor(s) will expect projects to demonstrate that the risks and policies outlined above have been addressed and implemented.

1554. **Assurance Levels**. There are, currently, no national guidelines on the assurance levels required for the gateway functionality of interconnected systems, except in the case of systems which have no constraint on the extent of access by users of one system to the other (Level 6). In such a case the two systems have to be integrated, conceptually, and an assessment made on the total system. Where systems are open to each other, but there are constraints (either technical or procedural) on the degree of access that one system has to another then a lesser degree of assurance may be appropriate. In no case, however, will this be less than the highest overall assurance level of the individual systems.

1555. **Maintenance**. In order for the security of the interconnected systems to be maintained, it is necessary to ensure that configuration management procedures are in place, so that the assertions and assumptions in the CoCo(s) or ISMS(s) are preserved. Accreditors will expect evidence that such procedures are in place, especially to cover issues such as additional connections.

Shared Data Environments

1556. As part of the Smart Procurement Initiative (SPI), the concept of Shared Data Environments (SDE) has been developed, which is based upon the interconnection of 3 or more domains to form an Extranet. The 3 types of domain involved in a SDE are :

a. MOD domain(s) ;

b. Shared domain(s) ;

c. External domain(s).

1557. Specific security advice for SDEs should be sought from DSy(Pol) before proceeding with any implementation.

Information Age Government

1558. As part of the Information Age Government (IAG) initiative, described in the Modernising Government White Paper in 1999, it is envisaged that Extranets will be formed linking departmental systems which provide electronic service delivery to citizens and businesses.

1559. It is recognised that certain specific security measures are required for such Extranets, as laid down in the Security Framework for IAG, Modernising Government Supplement 24, with the security requirements for those elements of the service contained wholly internal to Government remaining the remit of existing HMG Security Policy.

1560. The IAG recognises a number if different types of domain to form such Extranets:

a. Public Network Domain(s) (PND), which contain the part of the communications infrastructure that lies outside the control of the IAG operators and clients ;

b. IAG Service Provision Domain(s) (IAGSPD), which controls that part of the communications infrastructure that is under the service provider's control and is used to host the services ;

c. Departmental Service Provision Domain(s) (DSPD) which contains the CIS infrastructure that used to host all or part of a government service and is under the control of the department offering the service ;

d. Non-Departmental Service Provision Domain(s) (NDSPD) which contains the CIS infrastructure that used to host all or part of an IAG service supported by a non-departmental body and is under the control of the organisation offering or contributing to an IAG service ;

e. Client Network Domain(s) (CND) is that element of contains the CIS infrastructure under the control of the client that used to support access to government services. At the simplest, this can be a single domestic PC ;

f. Client Side Service Domain(s) (CSSD) is that element of the CIS infrastructure that is supplied by or on behalf of IAG services and installed within the CND to incorporate some important trust elements ;

g. Trusted Service Provider Domain(s) (TSPD) is that element of the IAG service that is operated under a service agreement on behalf of government by s commercial service provider.

1561. Specific security advice for implementing IAG services within MOD must be sought from InfoSy(Tech) before proceeding with any implementation.

Incident Handling

1562. As part of the Accreditation process, evidence will be required that management procedures are in place to detect and respond to any incidents affecting all MOD systems party to the connection(s) are in place, in accordance with **Chapter 11**. The preferred solution is for all SMIs to be directly or remotely accessible by protected means from a recognized Monitoring and Reporting Centre (MRC) with 24 hour coverage.

ANNEX A TO CHAPTER 15

BARRIER FUNCTIONS (BF) EFFICACY OF PROTOCOL CONTROLS

1. Based upon the current state of security technologies, the table overleaf indicates the efficacy achievable for various combinations of IP related protocols and Barrier Functions (BF). The assessed efficacy is an indication of that currently felt to be achievable at the current state of the art, and is expressed in terms of:

a. COTS – Possibly available from Commercial Off The Shelf (COTS) products;

b. GF – Possibly available from Government Furnished (GF) items, which includes:

(i) Government Off The Shelf (GOTS) products;

(ii) GF Toolkits;

(iii) Bespoke developments.

c. N/K - Not Known indicates that the protocol has been identified for investigation, but that no conclusion had been reached at the time of publication;

d X – a cross indicates that an acceptable level of security cannot be achieved for that protocol and hence should not permitted to traverse an SMI.

2 The assessment is the maximum efficacy believed to be implementable, and the proof of such a claim will normally require Evaluation or other forms of testing before being accepted as evidence for Accreditation.

3 Where a protocol is not referenced, this indicates that no Information Exchange Requirements (IER) have been identified for that protocol, and therefore that the issue has not been investigated either by MOD under Applied Research Package 13 (ARP13) or by CESG as the National Technical Authority. If IERs are discovered which need additional protocols to those laid down in this Annex, these should be notified at the earliest possible opportunity to both InfoSy(Tech) and EC(CCII)IOCM/Proj1 so that appropriate research can be initiated.

4. Due to the dynamic nature of the technologies and vulnerabilities involved, the relevant PSyA or the DSSO should be consulted before proceeding on the basis of this

information in case any updates have subsequently occurred.

Exchange Requirement	Barrier Function Efficacy			
	BP	EP	HP	SP
	Barrier Function Placements			
	Transport	Transport + Format	Transport + Format + Content	Transport + Format + Content + Interactive
ICMP	COTS	GF	GF	X
NTP and SNTP	N/K	N/K	N/K	N/K
Other Time Protocols (e.g. GPS)	N/K	N/K	N/K	N/K
SMTP	COTS	COTS	COTS	GF
X.400	COTS	COTS	COTS	GF
HTTP - Browse Down[1]	COTS	COTS	COTS	X
HTTP - Browse Up[2]	COTS	COTS	X	X
HTTPS	COTS	X	X	X
FTP - Connect Up[3]	COTS	COTS	GF	X
FTP - Connect Down[4]	COTS	COTS	GF	GF
NNTP	N/K	N/K	N/K	N/K
IMPP/MSNP(1863/TCP)	N/K	N/K	N/K	N/K
LDAP/X.500 – Server Only	COTS	COTS	X	X
DNS – Server Only	COTS	COTS	N/K	N/K
SNMP versions 1 and 2	X	X	X	X
SNMP version 3	COTS	COTS	GF	N/K
OTH-Gold	GF	GF	N/K	N/K
H.323/T.120 Video	X	COTS	X[5]	X
H.323/T.120 Document transfer	X	COTS	GF	GF
ICA	COTS	X	X	X
RDP	COTS	X	X	X
CORBA (end to end)	N/K	N/K	N/K	N/K
MDX + Other Proprietary	N/K	N/K	N/K	N/K

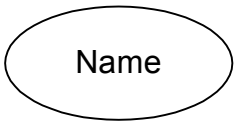
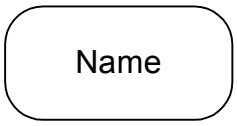
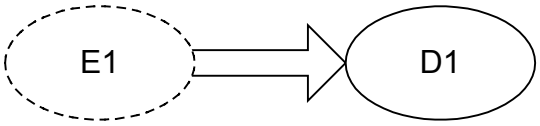
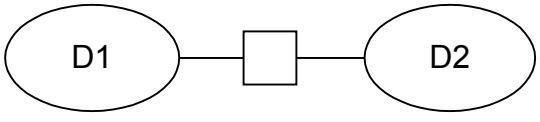
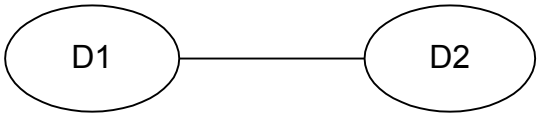
[1] This is when a browser is invoked from a high domain in order to view the web server contents of a lower domain.
[2] This is when a browser is invoked from a low domain in order to view the web server contents of a higher domain.
[3] This is when the original connect request is initiated from a low domain to a higher domain.
[4] This is when the original connect request is initiated from a high domain to a lower domain.
[5] An interactive control may be achieved on call setup.

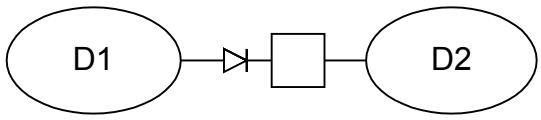
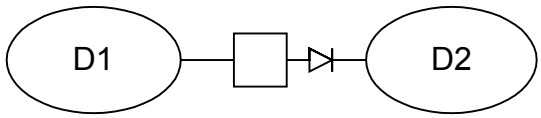
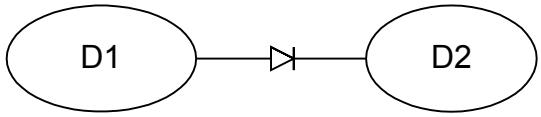
ANNEX B TO CHAPTER 15

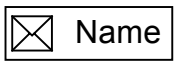
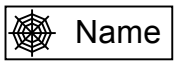
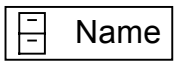
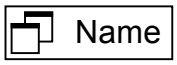
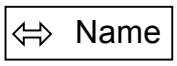
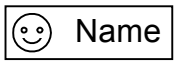
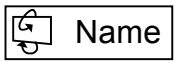
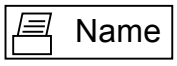
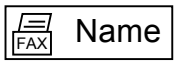
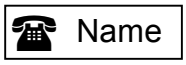
DOMAIN BASED NOTATION (From DERA Applied Research Package 21.c)

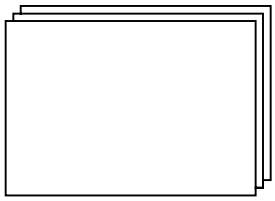
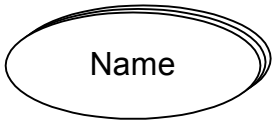
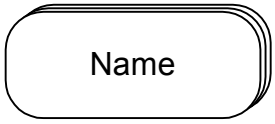
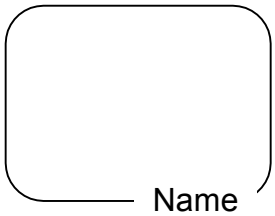
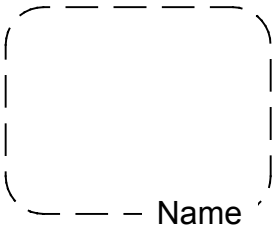
1. The symbols used in a domain model are all shown in this quick reference guide.

2. The symbols in the table are included as separate 'pictures', so that they can be copied from an electronic version of this document using 'cut and paste'. Alternatively, a Visio template is available for creating domain model diagrams with the Visio tool.

Basic elements	
	**Internal domain**
	**External domain**
	**Environment**
	**Portal**
Summary connections (connections of undefined type)	
	**Two-way**
	**One-way**

	**One-way** (D1 may only send) uses a diode symbol on the line:-
	**One-way** (D2 may only receive)
	**One-way** (D2 may only receive)

Connection types			
Message connection type			
	**or**		**Person to person messages**
Shared repository types			
	**or**		**Web site**
	**or**		**Filestore**
	**or**		**Database**
	**or**		**File transfer folder**
Conferencing types			
	**or**		**Video-conferencing**
	**or**		**White-boarding**
Miscellaneous connections			
	**or**		**Printing**
	**or**		**Fax**
	**or**		**Telephone**
Unconstrained connection type			
	Used when domains are mapped onto an architecture model, to connect two parts of a single, logical domain.		

Cloning	
	**Clone zone** Encloses any domain model element. Indicates replication of all model elements inside the zone.
	**Set of internal domains** Represents a number of domains that all have the same properties
	**Set of external domains** Represents a number of environments that all have the same properties
Refinement	
	**Refined domain** Encloses any number of component domains and connections, showing how they relate to a higher level view.
	**Refined environment** Encloses any number of component environments, showing how they relate to a higher level view.

ANNEX C TO

CHAPTER 15

DESCRIPTION OF IT SYSTEM INTERCONNECTION LEVELS

(FROM NATO INTEROPERABILITY PLANNING DOCUMENT WP 71-76 OF FEB 93)

1. Level 1 Interconnection.

a. **Application**.

(1) Level 1 is for systems closed to each other (either as a result of an operational decision, or as a result of a technical constraint), which require, to interoperate, a human interface and an associated off-line communications system with commonly accepted procedures.

(2) Level 1 is mainly applied to facilities that have no information systems.

b. **Concept and Characteristics**.

(1) Level 1 is completely manual, based on a message exchange concept between operators at each of the interoperating facilities using a communications system which is totally independent of either of any information system at either end. The essential characteristic of level 1 is this operator-to-operator off-line data transmission system.

(2) The information to be exchanged must be put into the agreed format for the communications by one operator, and sent to the other operator in accordance with agreed procedures. Each operator will be responsible for the retrieval or input of data from or to his local system.

(3) The information systems, where they exist, play no part in level 1 interconnection, and no standardization of systems is required. However, the use of common message standards considerably enhances the understanding and usability of the transfered information.

c. **Operating Process**.

(1) The analysis of information flow from system A to system B is as follows:

(a) The operator at system A interrogates the input/output device connected to system A. Access constraints will permit access only to that data to which he is authorised.

(b) The operator identifies the data required for dissemination to system B.

(c) The operator interprets the data by:

i identification of changes of message standard, format etc. as required by the common communications procedures;

ii verification of distribution and access rights;

iii verification of protective marking and other security constraints.

(d) The operator establishes communications with the operator at system B and passes the information to him in the agreed format. The operator at system B will acknowledge receipt.

(e) Operator B interprets the received data by:

i identification of changes of message standard, format etc. as required by system B;

ii verification of message validity and security constraints.

(f) Operator B interrogates the input/output device for system B and inputs the information in the correct format into system B.

The dissemination of data from system B to system A follows a identical pattern.

(2) Differences in vocabulary, and differences in the formats of messages and data in the two systems and the common communications

system, can interfere with information exchange between dissimilar systems.

d. **Security Aspects**.

(1) Human procedures will provide the primary constraints on interoperability in accordance with the operational and security requirements. These will be supplemented by some hardware and software controls on the access of the operators to their local systems.

(2) A key aspect of level 1 interconnection is the definition of the access rights of the interoperability operators to their own local system. Neither operator has any access to the other system.

2. **Level 2 Interconnection**.

a. **Application**. Level 2 is for systems closed to each other (either as a result of an operational decision, or as a result of a technical constraint), which require, to interoperate, a human interface belonging to each of the two systems.

b. **Concept and Characteristics**.

(1) Level 2 is also completely manual, but the independent communications link required for level 1 is eliminated. It is replaced by a liaison team from each facility, co-located in the other facility.

(2) Each liaison team has a terminal and means of communications for linking that terminal to its own system. The essential characteristic of level 2 is the co-location of system access devices and operators for each system; the systems are not electronically connected, nor does an operator from one system have direct access to the other system.

(3) Information is exchanged between the local operator and an operator of the liaison team, this presupposes that they are able to understand each other. The liaison team operators transform the information received from their hosts into a form acceptable to their own system.

(4) Whilst the use of common message standards is not a prerequisite for level 2, its use would considerably facilitate the work of the liaison teams.

c. **Operating Process**.

(1) The analysis of information flow from system A to system B is as follows:

(a) The operator at system A interrogates the input/output device connected to system A. Access constraints will permit access only to that data to which he is authorised.

(b) The A operator identifies the data required for dissemination to system B.

(c) The operator interprets the data by:

i identification of changes of message standard, format etc as required by the common communications procedures;

ii verification of distribution and access rights;

iii verification of protective markings and other security constraints.

(d) The operator passes the information to the system B liaison team operator.

(e) The system B liaison team operator interprets the data by:

i identification of changes of message standard, format etc, as required by the common communications procedures;

ii verification of distribution and security constraints.

(f) Operator B interrogates the input/output device for system B and inputs the information in the correct format into system B. He either:

i adds the database integrity parameters and access right controls required by system B; or:

ii inputs the data into a slave copy in system B in the required format, and the system manager of system B validates the information, adds database integrity and access right controls and updates the system B database from the slave copy.

The dissemination of data from system B to system A follows an identical pattern. Both processes could be accomplished at a single site (i.e. no requirement for 2 liaison officers).

(2) Differences in vocabulary, and differences in the formats of messages and data in the two systems, can place restrictions on information exchange between dissimilar systems.

d. **Security Aspects**.

(1) Human procedures will provide the primary constraints on interoperability in accordance with the operational and security requirements. These will be supplemented by some hardware and software controls on the access of the operators to their local systems.

(2) A key aspect of level 2 interconnection is the definition of the access rights of the interoperability operators to their own local system. Neither operator has any access to the other system.

3. **Level 3 Interconnection**.

a. **Application**. Level 3 is for systems closed to each other (either as a result of an operational decision, or as a result of a technical constraint), which require, to interoperate, a human interface with commonly accepted procedures.

b. **Concept and Characteristics**.

(1) Level 3 consists of exchanging system terminals between the two operational facilities; at each end, two terminals are co-located with a single user or operator, each terminal being connected to its corresponding system.

(2) The liaison teams required for level 2 interconnection are eliminated in level 3. The essential characteristic of level 3 interconnection is the non-physical connection of systems with a single operator for each interface between the interoperating systems. The operators are given access authorization to both systems, restricted to that necessary for them to perform their operational function.

(3) The level 2 co-located operators should be replaced by automated aids which help the operator in each system to put the information required from his own system into a form acceptable to the other system. This is necessary when both systems use different data access standards and different data presentation standards. Each system must use a standardised format for data presentation so that the automated aids can translate efficiently the data from one format to the other.

(4) The use of a unique standard message text format would considerably facilitate the work of the operator for transferring information from one system to the other.

c. **Operating Process**.

(1) The analysis of information flow from system A to system B is as follows:

(a) The operator interrogates the input/output device connected to system A. Access constraints will permit access only to that data to which he is authorised.

(b) The operator identifies the data required for dissemination to system B.

(c) The operator interprets the data by:

i identification of changes of message standard, format etc, as required;

ii verification of distribution and access rights;

iii verification of protective marking and other security constraints.

(d) The operator interrogates the input/output device connected to system B and inputs the information in the format required by system B.

(e) Either:

i the operator adds the database integrity parameters and access right controls required by system B; or:

ii the operator inputs the data into a slave copy in system B in the required format, and the system manager of system B validates the information, adds database integrity and access right controls and updates the system B database from the slave copy.

The dissemination of data from system B to system A follows an identical pattern. Again, both processes could happen at a single site, if the operator had the correct access permissions.

(2) It should be noted that differences in vocabulary can place restrictions on information exchange between dissimilar systems.

d. **Security Aspects**.

(1) Software, hardware and human procedures will provide the necessary constraints on access to control the input and output of data to limit interoperability in accordance with the operational and security requirements.

(2) A key aspect of level 3 interconnection is the definition of the access rights of the interoperability operators to each of the two systems.

4. **Level 4 Interconnection**.

a. **Application**. Level 4 is for two systems which are open to each other, but which have predetermined and fixed technical access constraints exist on the extent of the access by each system to the other.

b. **Concept and Characteristics**.

(1) Level 4 represents the lowest of the levels of interconnection based on a physical electronic connection between the two systems.

(2) Level 4 provides for the controlled availability of a limited subset of information within one system to users of another system, based on a predetermined restriction which may be as a result of a deliberate limitation imposed by operational requirements, or as a result of a technical limitation due to the incompatible design of the two systems. The essential characteristic of level 4 is the predetermined nature of these access constraints; they may be supplemented by additional dynamically controlled access constraints similar to those described under level 5.

(3) The availability of any of the subset of information will be subject to the individual users access rights.

(4) Because of the fixed and predetermined nature of the access constraints, changes to those constraints will involve some form of redesign or physical modification of one or both systems.

(5) The interface between the two systems is fully automated, and permits the exchange of information, within the limited subset, without the intervention of any operator of either system. However, it will be necessary for the two systems to have a common understanding of each other's access controls and information integrity criteria and parameters,

as well as the definition of the information subset that can be exchanged. It will also be necessary for some technical parameters to be aligned. Differences in any of these controls, criteria and parameters will impose limitations on the extent to which they systems may interoperate.

(6) It is a prerequisite for two systems that are required to interoperate at level 4 that they must adopt, for the limited subset of information to be exchanged, a common message standard so that translation from one internal format to the other can take place at the interface. A common data definition language for the limited subset of information to be exchanged will facilitate the translation process.

(7) Level 4 interconnection does not affect any national doctrinal requirements for the authorization of information prior to release.

c. **Operating Process**.

(1) Procedural standards must be defined for the two interoperating systems; "inter alia", these standards must define whether the transfer of information is to be performed on a "push" or "pull" basis. In the former case, all accesses to information by a user of a system will be satisfied from within the local data base of that system, irrespective of the original source of the information. In the latter case, any request for data held in the other system will cause a remote request to be generated, which will be satisfied by the other system. An agreed procedure may incorporate both "push" and "pull" mechanisms.

(2) The definition of the information subset resulting from the predetermined access constraints, and the definition of the access rights of individual users, will not be affected by the definition of the access mechanisms to be employed.

(3) Under normal circumstances, the user will not be aware of the mechanism being used to satisfy his request. The user will employ his normal information retrieval or request procedures for access to all information to which he has access rights.

d. **Security Aspects**.

(1) Software and hardware and human procedures will provide the necessary constraints on access to control the exchange of information, to limit interoperability in accordance with the operational and security requirements.

(2) A key aspect of level 4 interconnection is the definition of the access rights of the users to the subset of information provided by the other system.

5. **Level 5 Interconnection**.

a. **Application**. Level 5 is for two systems which are open to each other, and which conform to minimum standards for information definition and transfer such that there are no fixed constraints on the extent of access by users of one system to the other, but dynamic constraints are applied to each systems, in accordance with the current operational situation, such that only a user-defined subset of the total information base of one system is available to the other.

b. **Concept and Characteristics**.

(1) Level 5 represents the normal level of interconnection based on a physical electronic connection between two systems. It requires a greater measure of adoption of common standards for the definition and transfer of information by the two systems than with level 4, but provides, as a benefit, the ability for the users of a system to determine dynamically the extent of their own information that they wish to share with other systems and users.

(2) Level 5 provides for the dynamically controlled availability of a subset of information within one system to users of another system, limited by restrictions determined and defined from time to time by the commander of that latter system or his staff, which will be imposed or relaxed as the need requires a result of political or operational requirements. There are no predetermined technical constraints limiting the extent of information exchange.

(3) The specific availability to an individual user of any part of the dynamic subset of information currently made available between the systems will be subject to that particular users access rights.

(4) Because there are no fixed or predetermined access constraints, changes to the dynamic constraints will not involve any redesign or modification of either system.

(5) The interface between the two systems is fully automated, and permits the exchange of information, within the defined subset, without the intervention of any operator of either system. However, it will be necessary for the two systems to have a common understanding of each others access controls and information integrity criteria and parameters,

as well as the definition of the information subset that may be subject to exchange. It will also be necessary for some technical parameters to be aligned. Differences in any of these controls, criteria and parameters will impose limitations on the extent to which the systems may interoperate, and may reduce the interconnection to level 4.

(6) It is a prerequisite for two systems that are required to interoperate at level 5 that they must adopt a common message standard for any subset of information to be exchanged, so that translation from one internal format to the other can take place at the interface. This process is significantly eased if the two systems employ a common data definition language.

(7) Level 5 interconnection does not affect any national doctrinal requirements for the authorization of information prior to release.

c. **Operating Process**.

(1) Procedural standards must be defined for the two interoperating systems, including the information transfer and access mechanisms and procedures. More than one mechanism may be in force at any time.

(2) The definition of the information subset resulting from the dynamically determined access constraints, and the definition of the access rights of individual users, will not be affected by the definition of the access mechanisms to be employed.

(3) Under normal circumstances, the user will not be aware of the mechanism being used to satisfy his request. The user will employ his normal information retrieval or request procedures for access to all information to which he has access rights.

d. **Security Aspects**.

(1) Software, hardware and human procedures will combine to provide for the dynamic determination and definition of the access constraints required at any time. Software and hardware will implement the necessary constraints on access to control the exchange of information to the limits thus defined, and to limit interoperability in accordance with the operational and security requirements.

(2) A key aspect of level 5 interconnection is the definition of the access rights of the users to the information provided by the other system, irrespective of definition of the current subset.

6. **Level 6 Interconnection**.

a. **Application**. Level 6 is for two systems which are open to each other, which conform to minimum standards for information definition and transfer, and for which there are no constraints on the extent of access by users of one system to the other; the two systems thus appear to both sets of users to be a single system. It is likely that such situations will only apply to two systems within a single command, or between two systems of a single nation.

b. **Concept and Characteristics**.

(1) Level 6 represents the highest level of interconnection between two systems. It is equivalent to level 5 interconnection with all dynamic restrictions removed. It requires a total adoption of common standards for the definition and transfer of information by the two systems.

(2) Level 6 provides for the total availability of all information within one system to users of another system without restrictions. There are no technical constraints limiting the extent of information exchange.

(3) The specific availability to an individual user of any information from either of the systems will be subject to that particular users access rights.

(4) The interface between the two systems is fully automated, and permits the exchange of any information without the intervention of any operator of either system. However, it will be necessary for the two systems to have a common understanding of each others access controls and information integrity criteria and parameters, as well as the definition of the information subset that may be subject to exchange. It will also be necessary for some technical parameters to be aligned. Differences in any of these controls, criteria and parameters will impose limitations on the extent to which the systems may interoperate, and may reduce the interoperability to level 4.

(5) It is a prerequisite for two systems that are required to interoperate at level 6 that they must adopt a common message standard for all information, so that translation from one internal format to the other can take place at the interface. This process is significantly eased if the two systems employ a common data definition language.

(6) Level 6 interconnection does not affect any national doctrinal requirements for the authorization of information prior to release.

c. **Operating Process**.

(1) Procedural standards must be defined for the two interoperating systems, including the information transfer and access mechanisms and procedures. More than one mechanism may be in force at any time. The definition of the access rights of individual users will not be affected by the definition of the access mechanisms to be employed.

(2) Under normal circumstances, the user will not be aware of the mechanisms and procedures. More than one mechanism may be in force at any time. The definition of the access rights of individual users will not be affected by the definition of the access mechanisms to be employed.

d. **Security Aspects**.

(1) Software and hardware will implement the necessary constraints on access to ensure that users cannot exceed their access rights, in accordance with security requirements.

(2) A key aspect of level 6 interconnection is the definition of the access rights of the users to the total of information provided by both systems.

ANNEX D TO CHAPTER 15

CALCULATION OF SECURITY FUNCTIONALITY REQUIRMENTS FOR INTERCONNECTIONS (From Hmg Infosec Standard No. 3)

1. A logical diagram of the connections to be analysed, including all known "cascade" connections, should be produced, using the Domain Notation as laid down at Annex B.

2. From this diagram, a series of abstract diagrams should be prepared, with each abstract centring on one domain under MOD control and showing all the other domains as an external domain. Straight line connections should be drawn from this "Protected" domain being analysed to all external domains (i.e. showing "full meshed" connection), and these should be numbered individually.

3. For each connection, determine the number of steps removed from the domain under consideration, which gives the "degrees of indirection":

Steps	Degree of indirection
1	Direct Connection
2	1 degree of indirection
3	2 degrees of indirection

4. Using these diagrams, the following methodology can be used to determine the Risk Profile of all connections.

5. A table listing all such connections should first be produced :

	C.1	C.2	C.3	C.4	C.5	. . . . .	C.n
Basic Risk Profile (BRP)							
Separation Modifier							
Accreditation Modifier							
Cascade Modifier							
Connection Risk Profile (CRP)							

6. Values for the assessment are given below :

Basic Risk Profile

7. Protective Marking Assessment

Summary of External Domain(s) or Intranet / Internet	**Highest Protective Marking in Protected Domain(s) or Intranet**				
	Unclassified	**Restricted**	**Confidential**	**Secret**	**Top Sercet**
TOP SECRET					1
SECRET			1	1	3
CONFIDENTIAL			1	3	5
RESTRICTED		1	3	5	7
UNCLASSIFIED	1	3	5	7	9

8. Criticality Level Assessment

Summary of External Domain or Intranet / Internet	**Highest Criticality Level of Protected Domain(s) or Intranet**			
	CL4	**CL3**	**CL2**	**CL1**
CL1				2
CL2			2	4
CL3		2	4	7
CL4	4	4	7	9

9. The Basic Risk Profile (BRP) is the highest number from either the Protective Marking or Criticality Level sections of the table :

Separation Modifier

Type of Separation Required on "Protected" Domain	**Modifier**
None	-1
Descriptors	0
Caveats	+1
Codewords at STRAP Equivalence Level (SEL) 1 or 2	+2
Codewords at STRAP Equivalence Level (SEL) 3	+3

Accreditation Modifier

Accreditation / Approval Rights from Protected to External Domains	Modifier
Joint Accreditation with Inspection Rights	-2
Joint Accreditation or Formal Memorandum of Understanding (MOU), but no Inspection Rights	-1
Adherence to common security standards (e.g. BS7799)	0
Otherwise	+1

Cascade Modifier

Degree of indirection from "Protected" Domain	Modifier
Direct Connection	0
1 degree of indirection	-1
2 or more degrees of indirection	-2

10. Having completed the table, the CRP for each connection is determined by summing the values. The worst case CRP for each domain is used to derive the requirement for security functionality within the Secure Managed Interface (SMI) on the boundary of the domain, using the following table :

CRP	SMI Functionality Required
≤ 0	No specific requirement, but Baseline Protection (BP) recommended
≥ 1	Baseline Protection (BP)
≥ 3	Enhanced Protection (EP)
≥ 5	High Protection (HP)
≥ 7	Special Protection (SP)
≥ 9	Special Protection (SP), subject to prior review and approval by DSy(Pol)
≥ 11	Security Control and Release Terminal (SRCT) or Cryptographic tunnel modes, subject to prior review and approval by DSy(Pol)

11. The functionality requirements for the different types of protection are given in **Chapter 15**.

This page is intentionally left blank

INTERNATIONAL COLLABORATION

This page intentionally left blank.

CHAPTER 16

INTERNATIONAL COLLABORATION

Introduction

1601. Security of IT Systems and networks whose components are geographically dispersed, under different jurisdictions, and hosted by a number of different nations and/or agencies cannot be easily managed. When operating in an international environment security requirements may be constrained upwards or downwards by the other partners. A Security Accreditation Panel should be established, comprising representatives of participating nations, responsible for endorsing the System Security Policy and identifying the security related documentation requirements for the IT systems or networks to be interconnected, and accrediting the systems and network interconnections. Specific guidance on the accreditation of NATO systems and networks is provided in NATO document AC/35-D/1021.

1602. This chapter provides core policy statements, which form the basis for the comparison of individual nations IT security policy, to determine if there are inconsistencies that may conflict when interoperable or joint systems are being considered. It provides a high level check-list rather than detailed policy. The security arrangements for the release of UK protectively marked information to Combined Joint Task Forces/Coalition missions, involving UK Armed Forces, are in **JSP 440 Volume 1 Chapter 11**.

1603. Annex A provides policy on the procedures in respect of the evaluation, certification and accreditation of IT systems and networks processing protectively marked information.

Definitions

1604. The following terminology may be encountered when dealing with International Collaboration programs:

a. **Shared Information Systems (SIS).** System(s), including interconnecting networks and supporting infrastructure elements, which process, store or transmit shared information; and over which participating member nations share responsibility for its operation;

b. **Affiliated Systems (AS).** Those systems or network components under a nation's or organization's management and control that process, store or transmit coalition information;

c. **Secure Managed Interface (SMI).** One or more 'Boundary Protection Devices (BPD) forming the control point(s) between SIS and AS, which could include "Security Release Control Tools" (SRCT), one-way or bi-directional multi-security level (MSL) devices, etc;

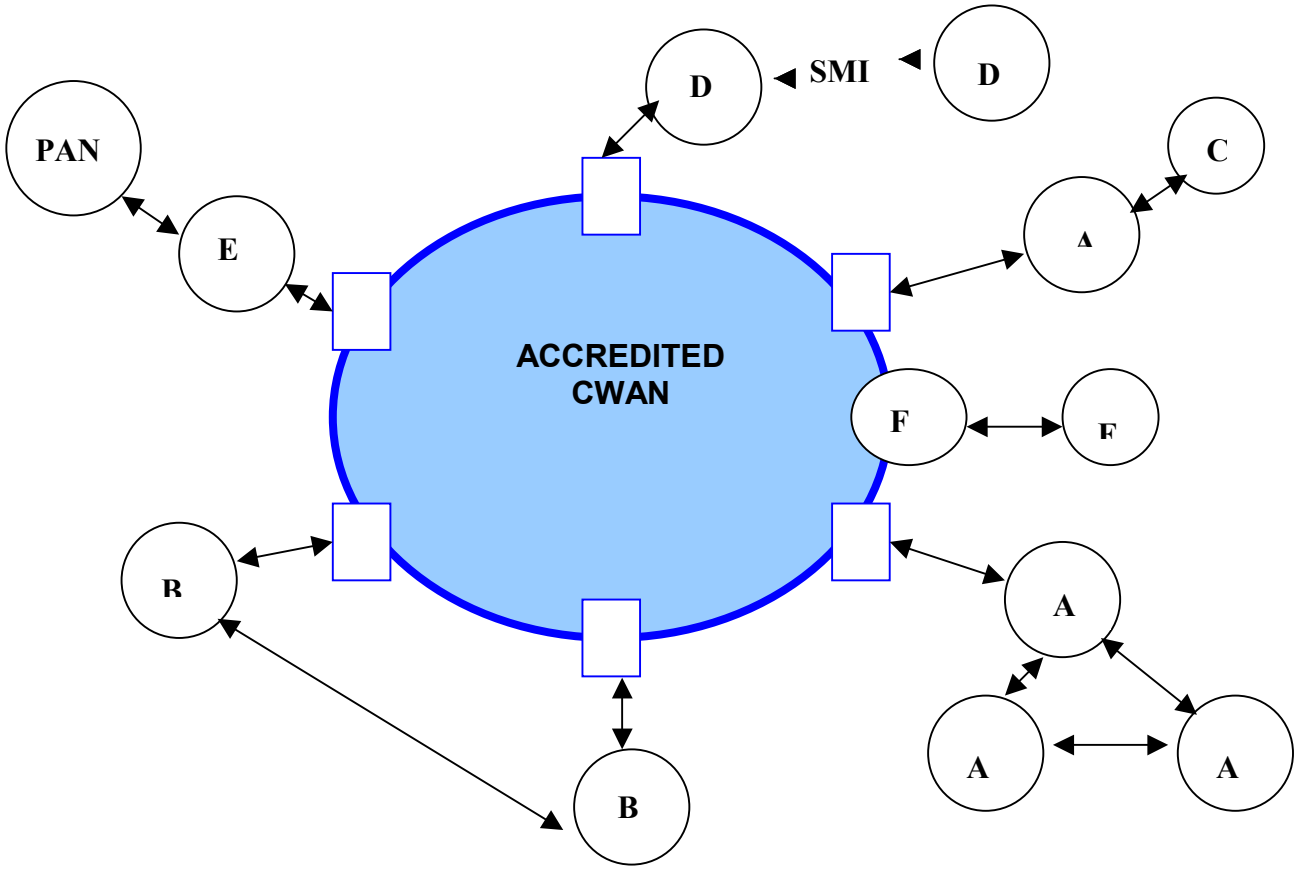
d. **Publicly Accessible Network(s)** (PAN), such as Internet;

e. **Designated Approving Authority (DAA) or System Approving Authority (SAA)**. The accreditor.

Interconnection Scenarios

1605. In addition to bilateral or multilateral connections using dedicated infrastructures, a growing number of coalition interconnections are achieved using shared infrastructures, often referred to as Coalition Wide Area Networks (CWAN).

1606. When interconnecting through a CWAN, the following specific security issues should be considered:



Scenario	Summary	Generic Security Issues
A	Connection of one or more AS and site, directly or indirectly, to the SIS Infrastructure.	• Mutual recognition of Accreditation of the nationally controlled AS
B	Connection of AS both through the SIS Infrastructure and between AS locations.	• Mutual recognition of Accreditation of the nationally controlled AS
C	Connection of one or more AS to an AS already connected to SIS Infrastructure.	• Mutual recognition of Accreditation of the nationally controlled AS
D	Connection of one or more AS already connected to SIS Infrastructure to National-only systems via a Nationally controlled Secure Managed Interface (SMI).	• Mutual recognition of Accreditation of the SMI as separating SIS Infrastructure from National-only systems
E	Connection from one or more AS connected to SIS Infrastructure to Publicly Accessible Network(s) (PAN), such as Internet.	• MSAB would always wish to be appraised of any PAN, irrespective of acceptance by Nation
F	Connection of one or more non-Core member to the SIS Infrastructure	• MSAB must endorse addition of more non-Core member(s) • Need to sanitize any Coalition data on shared Infrastructure that is not releasable to new member

Security Management Policy

1607. Requirement to Accredit. All IT systems are to be accredited. For each system the System Sponsor(s)/Owner(s) is to ensure that this occurs. IT systems may need to be reaccredited when the system configuration is changed from that which was previously accredited.

1608. Post Accreditation Audit. The national Defence Security Authority shall ensure that post accreditation auditing is conducted.

1609. Authority for Granting Waivers and Concessions. Only national Defence Security Authorities may grant waivers and concessions to national security policy.

1610. Aggregation of Information. The System Sponsor(s)/Owner(s) are to ensure that a periodic assessment is made of the sensitivity that results from aggregation of information processed by the system.

1611. Caveats, Codewords and Special Handling. Where an IT system processes information that is protected by a caveat, codeword or special handling, the System Sponsor(s)/Owner(s) are to consult with the relevant national Defence Security Authority, who may advise of security that is required in addition to that defined by this policy.

1612. Contingency Planning. For each IT system the System Sponsor(s)/Owner(s) are responsible for formulating, testing and maintaining a contingency plan.

1613. Use of Non-Defence Systems. In the exceptional cases where Defence information is processed on non-Defence IT systems, use of the systems must be approved by the national Defence Security Authority.

1614. Use of Defence Systems Outside a Defence Controlled Area. The use of a Defence IT system to process Defence information outside a Defence controlled area must be approved by the national Defence Security Authority.

Personnel Security Policy

1615. Clearances and Authorizations. The System Sponsor(s)/Owner(s) are to ensure that all users of the IT system have appropriate clearance, briefings and authorization to the highest level of data processed/stored by the IT system or commensurate with the Mode of Secure Operation.

1616. Passwords. Users are to ensure that passwords are protected outside the system to a level consistent with the classification of the system.

1617. Breaches of Security. Procedures must be in place for identifying, reporting and managing breaches of security.

1618. Classification by Users. Originators of information are responsible for the classification of that information.

Physical Security Policy

1619. Overall Physical Security. All physical security which is a part of an IT system is to be in accordance with participating member nations national policy and standards, as defined by their respective security authorities.

Software Security Policy

1620. Import of Information. The import of all information into a IT system from any source, either by media or a network connection to an external system, is to be approved in accordance with operating procedures. It is also to be legally acquired and used in accordance with the licence agreement.

1621. Malicious Software Protection. A malicious software strategy shall be maintained. All data shall be checked on export.

1622. Passwords. Passwords shall be used to support identification and authentication of users, there shall be a mechanism that protects the integrity of the password. The classification applied to a password will normally be the highest classification to which the password gives access.

Hardware And Media Security Policy

1623. Handling and Marking of Electronic Storage Media. All types of removable electronic storage media is to be labelled, handled, accounted for, de-classified or re-classified, and disposed of, in accordance with their security classification.

1624. On-site Maintenance of Classified Hardware and Media. If classified assets of a Defence information system is maintained on-site, the maintainer is to either hold a security authorization and/or clearance at the appropriate level, or be escorted by someone who is authorised and/or cleared.

1625. Off-Site Repair of Classified Hardware and Media. If classified assets of a Defence information system is repaired off-site, the removal and repair of the media is to be in accordance with 1621 above.

Network Security Management Policy

1626. Extent of Network Connections. The Sponsor(s)/Owner(s) are to obtain details of the extent of all connections, for inclusion in the system security policies and inform the Network Managers of onward connected systems.

1627. Degree of Access. The Sponsor(s)/Owner(s) are to establish a written understanding of the degree of access that users of the system will have to other connected systems.

1628. Access Control. The Sponsor(s)/Owner(s) are to determine the access controls that will be used to control users of the system when accessing the other connected systems.

1629. Network Management Disputes. The Sponsor(s)/Owner(s) are to establish a process by which dispute over network management issues can be resolved or be taken to a higher authority for resolution.

1630. Information Aggregation. The Sponsor(s)/Owner(s) are to recommend to the national Defence Security Authority, the information aggregation situations that may require a security classification higher than that of the individual information items to which access is allowed on the network.

Communications Security Policy

1631. Requirement to Protect Information During Transmission. All classified information is to be protected by either:

a. Government approved cryptography; or;

b. A protected distribution system.

Emanations Security Policy

1632. Tempest Threat Assessment.A Tempest threat assessment is to be undertaken for all Defence information systems, in accordance with national policy.

1633. Tempest Standards. The basis for Tempest standards within Defence is the relevant National Security Instructions.

ANNEX A TO

CHAPTER 16

MULTI-NATIONAL EVALUATION, CERTIFICATION AND ACCREDITATION PROCEDURES

Introduction

1. This Annex provides policy on the procedures in respect of the evaluation, certification and accreditation of IT systems and networks processing protectively marked information. (Hereafter referred to as systems). The procedures cover joint systems that are to be implemented by two or more nations and are required to be evaluated in accordance with national/international minimum standards.

2. Overall control of a joint development project or system will normally be under the control of a Joint Project Office (JPO) which will be responsible for appointing a multi-national security working group. The principles and processes set out below are intended to provide the basis for developing individual memoranda of agreement.

Basic Principles

3. Accreditation may need to be supported by evaluation and certification in accordance with national/international standards. When this is necessary each joint system with an IT security requirement shall be certified as required against Information Technology Security Evaluation Criteria (ITSEC) and the Information Technology Security Evaluation Manual (ITSEM), or Common Criteria by a Joint Certification Panel (JCP), comprising representatives from the participating nations.

4. When required by the system security policy, security products used in a system must have been evaluated against the ITSEC and ITSEM, or Common Criteria, by Information Technology Security Evaluation Facilities (ITSEFs) approved by the JCP.

5. The nations shall agree to the sharing of the evaluation results, provided that adequate evaluation competence can be demonstrated by a participating nation. Once demonstrated, their ITSEC product evaluation results may be reused in the system evaluations.

6. Copies of all evaluation documents and deliverables shall be distributed among the

other participating nations.

7. For systems comprising a number of subsystems there will be an option to set a maximum evaluation level for each subsystem. Exceptions can be made for precisely identified architectural components such as gateways. Any such changes are to be fully justified by the developer based on the application of HMG Infosec Standard No 1 (as amplified in **Chapter 6**), NATO AC/35-D/1023 or other national standards.

Evaluation Process

8. General Organisation. Evaluations may be carried out by a single nation ITSEF or by joint teams. Each nation may nominate evaluators to observe the general conduct of the system evaluations. These evaluators are termed "foreign auditors". The foreign auditors shall have the same access rights as members of the evaluation team. This shall include access to the evaluation premises, all evaluation deliverables, all evaluation correspondence, all evaluation outputs, all intermediate results and any evaluation meeting. Their work may include checking that evaluations are being completely undertaken by each evaluation team.

9. Joint Evaluations. There shall be an option for system evaluation work to be performed by fully integrated joint evaluation teams.

10. Numbers of Evaluators and Foreign Auditors. Each nation will be permitted to supply a number of evaluators in a joint evaluation team, which is in proportion to the total number of participating nations.

11. For any evaluation, the number of foreign auditors from a given nation shall total no more than two at any one time. At least one foreign auditor per evaluation per nation shall be permitted.

12. Funding. Each evaluation will normally be funded by the evaluation sponsor. Funding of certification fees will be negotiated on a case by case basis.

Certification Process

13. Joint Certification Panel (JCP). The JCP shall comprise representatives from the certification bodies of the participating nations. Each meeting of the JCP shall require at least one representative from each national Certification Body.

14. The Chairman shall be from the nation whose evaluation is under consideration, otherwise general meetings will be held on a rotational basis. The Secretary shall be from the host nation.

15. A JCP Interpretation shall agree any ITSEC/ITSEM, or Common Criteria interpretations for system evaluations.

16. Conduct of System Evaluation. Prior to the evaluation, the JCP shall approve the Evaluation Work Plan (EWP).

17. During the evaluation, the JCP shall review the conduct of the evaluation and determine whether the evaluation has met the requirements of ITSEC/ITSEM or Common Criteria.

18. If unanimous agreement cannot be achieved on the evaluation deliverables, the ITSEF's national Certification Body shall request appropriate additional evaluation deliverables.

19. If unanimous agreement cannot be achieved by the JCP on the EWP or the conduct of the evaluation, the ITSEF's national Certification Body shall request appropriate additional evaluation work.

20. The JCP shall approve the Evaluation Technical Report (ETR) and confirm the evaluation results.

21. The national Certification Body will issue, to the national Accreditation Authority and the JCP, a national certification report for the evaluated system.

22. A national Certification Body may also issue an endorsement (with any caveats) of a certification report received from another nation.

23. When the Security Accreditation Panel (or in the case of single national system implementations each national Accreditation Authority) has endorsed all national certification reports and has given its subsequent formal accreditation, this shall be the evidence to be presented by the JPO to the Joint Acceptance Committee as part of the overall Acceptance into Service process.

Document Distribution

24. The Joint Project Office (JPO) shall be responsible for ensuring that all required evaluation deliverables are produced by the evaluation sponsor and developer.

25. The national Certification Body shall be responsible for arranging distribution of the Evaluation Technical Report(s), the Certification report(s) and any related documents to the certification bodies of the other nations.

This page intentionally left blank.

INTRODUCTION TO COMMUNICATIONS AND ELECTRONIC SECURITY

This page intentionally left blank.

CHAPTER 17

INTRODUCTION TO COMMUNICATIONS AND ELECTRONIC SECURITY

Applicability

1701. Line Managers are responsible for ensuring that staff under their control are briefed in the use of communications and electronic systems for passing protectively marked information as laid down in this JSP.

Aim

1702. The term InfoSec is used to describe the Technical Facets of Security, which encompass the disciplines of CompuSec, RadSec and ComSec. The aim of this Part is to state the ComSec and RadSec regulations and practices that will be encountered in the working environs of the MOD and associated establishments. The issue of CompuSec is discussed in detail at **Part 1**.

Communications Security (Comsec)

1703. Foreign intelligence services (FIS) are continuously at work collecting information of intelligence value. They have considerable expertise in the interception of radio, telephone and data communications and this underlines the need for the highest standards of security in this field.

1704. Communications security (ComSec) is the collective title for measures taken to protect all aspects of communications to deny access to information of value which might be derived from a study of communications material and information to unauthorised persons, or to mislead authorized persons in their interpretation of the results of such a study. ComSec has 4 components:

a. **Physical Security - including Document Security**. Physical security is that component of ComSec which results from the physical security measures necessary to protect all types of ComSec material from surreptitious attack by FIS, or any access by unauthorized persons.

b. **Personnel Security**. The aim of personnel security is to provide an acceptable level of assurance of the integrity of personnel given access to ComSec activity and information.

c. **Cryptographic Security (Cryptosecurity)**. Cryptosecurity is that component of ComSec which results from the provision of CESG approved cryptosystems and their proper use. The correct application of cryptosecurity

provides the defence against cryptanalysis.

d. **Transmission Security (TranSec)**. TranSec is that component of ComSec which results from all measures designed to protect transmissions from unauthorized interception, traffic analysis and imitative communications deception. For Further details see **Annex A**.

1705. The current MOD policy is therefore that for all operational military communications should be carried out in accordance with the communications procedures laid down in Allied Communications Publications (ACPs), as supplemented by Defence Communications Publications (DCPs), in conjunction with the Security Requirements laid down in this Manual.

1706. All users of communications systems are to have a working knowledge if the relevant publications, and to be trained in the correct use of the procedures adopted therein. The adherence to the authorized procedures allows military communications to be established, and information transmitted, rapidly and concisely, and reduces the opportunity for misunderstanding, which materially improves ComSec, and the efficiency and reliability of communications.

The Threat From Signal Intelligence (SIGINT)

1707. In order to appreciate the importance of maintaining high standards of ComSec it is necessary to understand the implications of SIGINT. SIGINT is information gained from the interception and analysis of another nation's electronic communications transmissions.

1708. The techniques for obtaining information in this way are well known and it must therefore be assumed that our communications are under constant study by foreign intelligence agencies. In addition there is always the possibility of the exploitation of this source of information by subversive organizations, and on occasions by the press and public.

1709. In wartime the SIGINT achievements of an enemy organization may be demonstrated dramatically by rapid success in battle. In peacetime, however, the efforts will not be so readily identifiable but will provide the enemy with the opportunity to build up a dossier of wide ranging and valuable information. In the subsequent event of war such information, combined with information from other sources, will provide high grade intelligence which could be of immediate benefit to the enemy.

Radiation Security (RADSEC)

1710. Radsec is that component of INFOSEC which results from the measures necessary to deny to unauthorized personnel information of value which might be derived from the interception and analysis of compromising emanations from communications/electronic equipment. It includes the discipline of TEMPEST.

1711. Detailed advice on RadSec is given at **Chapter 21**.

Roles and Responsibilities

1712. Details of specific roles and responsibilities for aspects of ComSec and RadSec are laid down in the relevant Chapters. In the context of the Department as a whole, the following roles are defined :

a. **Defence ComSec Authority** The overall responsibility for ComSec within Defence rests with the Departmental Security Officer (DSO). The formulation and promulgation of Defence ComSec Policy is delegated to InfoSy(Tech) within DDefSy, who therefore acts as the Defence ComSec Authority ;

b. **Defence ComSec Operating Authority** The responsibility for overall co-ordination and implementation of ComSec operational issues within Defence is delegated by the Defence ComSec Authority to a nominated Defence ComSec Operating Authority, currently DCSA IA Branch ;

c. **Defence Radsec Authority** The overall responsibility for RadSec within Defence rests with the Departmental Security Officer (DSO). The formulation and promulgation of Defence RadSec Policy is delegated to InfoSy(Tech) within DDefSy, who therefore acts as the Defence RadSec Authority ;

Installation Control

1713. In order to maintain the security of CIS, good installation practice is required, in terms of both initial fit and configuration management throughout life.

1714. Enforcement is primarily carried out by the process of Installation Design, which must be obtained before any CIS is permitted to store, process or forward any official information. The issue of an Installation Design Conformance Certificate verifies for the Data Owner(s) that implementation does not present an unacceptable Confidentiality risk to the Information being processed, and also confirms, for the System Management authority, that appropriate asset protection for Integrity and Availability is in place.

1715. To the extent to which systems fall completely within their area of responsibility, the control of this subject is vested in the designated Coordinating Installation Design Authority (CIDA), who are acting as the agent of the DSSO or TLB PSyA in the discharge of security relevant aspects of their duties. Details of the CIDAs are given at **Annex C to Chapter 21**.

1716. The appropriate CIDA for a site or system is determined from the organisation responsible for security for the site or platform.

1717. The role of CIDA must be performed by a member of MOD staff.

1718. Details as to the subordinate staffs within Sectors tasked with performing elements of IT and communications system/installation Design Control are laid down in the RadSec element of this **Volume, Chapter 21**.

Operations Security

1719. The topic of Operational Security (OpSec) is addressed in more detail **at Volume 1,** but in the context of communications security it is particularly important to consider OpSec where the subject matter is notionally UNCLASSIFIED, as inferences can be drawn from operator chatter and mannerisms, use of jargon, and call signs. The following will be the main areas requiring a specific OpSec assessment.

1720. **Engineering Order Wires** In many communications installations, unprotected links are provided for circuit engineering purposes, which may be carried by a variety of means including radio links. These are generically referred to as Engineering Order Wires (EOW). It is important that good communications discipline be exercised in the use of these EOW circuits, which are only to be used for UNCLASSIFIED purposes.

1721. **Test Tapes** It is essential that where the same test tapes are frequently used in conjunction with a cryptosystem (e.g. within ACP127 messaging), that the agreed, standard test tape is used rather than "home made" test tapes, however humours they may be, as the standardised for has been proven to both exercise all the functions of the equipment, and not to have any non-standard formatting or errors that would allow indentification of Service, formation, or unit involved.

1722. **Administrative Communications** Experience has shown that notionally UNCLASSIFIED, administrative communications concerning such matters as supply problems, technical matters and even social events such as cocktail parties and sports fixtures can be used to provide intelligence on future operational activities, and can also be of interest to terrorist organisations. In particular, where communications relate to the movements of Senior Officers and VIPs, consideration should be given by originators as to whether a Protective Marking is actually required in order that appropriate ComSec measures are used.

ANNEX A TO CHAPTER 17

TRANSMISSION SECURITY

Introduction

1. Transmission Security (TranSec) is the element of ComSec which addresses the following:

a. **Unauthorized Interception**. The act of searching for, listening to and/or recording communications for the purpose of obtaining intelligence ;

b. **Traffic Analysis**. The study of external characteristics of communications to obtain intelligence from the nature of the traffic ;

c. **Imitative Deception**. The introduction of spoof transmissions in order to deceive, confuse or overload communications, break down ComSec or influence the course of operations.

Countermeasures

2. TranSec measures are designed to obstruct enemy attempts to disrupt or gather intelligence from our use of communications. These measures include the following:

a. **Traffic Flow Security (TFS)**. TFS disguises the characteristics of communications which would otherwise provide intelligence to an enemy. This includes the use of dummy traffic to hide the nature, distribution, frequency and significance of genuine traffic.

b. **Frequency Hopping**. Changing the transmission frequency, according to a predetermined pseudo-random pattern, frustrates interception and spot-jamming of transmissions.

c. **Spectrum Spreading**. Use of spread spectrum techniques increases the complexity of transmission jamming and interception. It also reduces the power radiated on any given frequency.

d. **Encryption**. Encrypting transmissions denies the enemy the intelligence to be gained from message content. Some types of cryptographic equipment have a TFS facility embodied.

e. **Training and Education**. The Unit OPSEC Officer is responsible for advising on TranSec matters and raising Unit awareness of TranSec issues,

particularly the dangers inherent
in plain language transmissions. Significant training opportunities can be gained from the monitoring of TranSec during exercises.

f. **Transmission Discipline**. Keeping transmissions to the minimum length and distribution, and ensuring brevity and clarity will minimize the opportunities for interception and possible linkages between messages. Message originators should be aware of the protective marking of aggregated information in transmissions and the intelligence to be gained from patterns of transmissions. Radio operators should observe the radio transmission protocols and the use callsigns.

g. **Authentication**. Message originators and recipients should use approved authenication mechanisms to frustrate deception attempts.

h. **Codes**. Particularly when using unprotected transmission media, it is important to recognize essential elements of friendly information and use approved encoding mechanisms, such as NATO Combat Codes, where appropriate.

i. **Defensive Monitoring**. Regular assessment of TranSec by defensive monitoring exercises and live transmissions provides feedback as to the effectiveness of the TranSec measures. Effective follow up of TranSec breaches also aids the education process.

TELEPHONE SECURITY

This page intentionally left blank.

CHAPTER 18

TELEPHONE SECURITY

Protectively Marked Speech over Telephones

1801. No telephone system, whether it be MOD, Government or Public Telephony Operator (PTO) provided, is fully secure, and calls are vulnerable to interception and overhearing., although the following non-security factors do provide some element of protection :

a. *Dilution Effect*. It is technically difficult and expensive to identify and extract particular telephone calls when they are 'mixed-in' with the myriad of telephone calls that make up the rest of Telephone Networks at any one instant.

b. *Dispersion Effect*. The dynamic routing of calls over Telephone Networks further complicates the targeting of particular traffic since a call between two points, if repeated, is unlikely to be routed via the same channel on both occasions.

c. C*ompression and Multiplexing*. Most communications media incorporate features enabling the maximum amount of data to be sent down a given channel. Compression and multiplexing techniques are often applied to communication channels to eliminate the otherwise redundant capacity taken up by the natural pauses in conversation, thereby achieving a higher capacity network. Though utilised for mainly commercial reasons, such features deter casual access to the information being passed and thus afford a further degree of inherent security.

1802. Telephones are vulnerable in the following ways:

a. **Casual overhearing.** This is overhearing by persons nearby the telephone instrument being used, or those who may have access to the communications path, such as switchboard/helpline operators, technicians, linesmen or other subscribers (by cross connection, feature interaction or induction). If the matter overheard is interesting enough, this may thereafter encourage deliberate eavesdropping ;

b. **Deliberate interception.** This is intentional, planned interception by foreign intelligence services, subversive organizations or militant members of protest, nationalist organisations, and members of the press. The techniques involved include the use of covert eavesdropping devices and hacking into telephone switch software.

1803. Microwave circuits may be used for long distance and some local telephone calls in place of conventional cable circuits. Subscribers will not normally be aware that their calls are being routed over microwave links. Such links can be intercepted from numerous places including foreign diplomatic premises both within the UK and overseas.

Protection of Telephone Calls

1804. The following defines the requirements for the protection of telephone conversations:

a. **TOP SECRET.** TOP SECRET telephone calls must **always** be made over cryptographically protected secure systems ;

b. **SECRET AND CONFIDENTIAL.** SECRET and CONFIDENTIAL telephone calls should be made over secure cryptographically protected systems, unless the telephone exchange is MOD operated, and has been Accredited for passage of SECRET between directly connected extensions. In all such cases, the Accreditation process must involve the DSSO, and be carried out in accordance with Annex A.

c. **RESTRICTED.** Telephone networks in mainland UK are approved for telephone calls up to and including RESTRICTED without additional countermeasures. Calls to, from and outside mainland UK are limited to UNCLASSIFIED only, RESTRICTED or above calls must be made over encrypted links.

Procedural Security Aspects

1805. The requirements for technical countermeasures are supplemented by procedural protection in the form of rules for users of telephone systems. These rules, which place responsibility for safe use of the telephone on the user, are:

a. No protectively marked information is to be disclosed to an unknown caller. If in doubt or where there are suspicious circumstances the caller should be asked to give a telephone number at which he can be rung back. This number should be checked from a telephone directory or with the organisation whom the caller claims to represent before any official information is disclosed. If necessary, users will first obtain formal authentication.

b. When establishing a call in which protectively marked information is to be discussed it is the responsibility of the calling party to satisfy himself that the recipient is *bona fide*. The communications system in itself will not always be an adequate safeguard for this purpose, and it is stressed that even for some modern systems which provide visible authentication of the connected terminal

equipments themselves, this cannot be taken to provide any significant measure of authentication of the actual user of the equipment during a given call;

c. The use of guarded language (veiled speech) to protect protectively marked information is at best unsatisfactory and should only be employed in emergencies;

d. If during the period of a call, if either caller recognises the other party is raise the level of the conversation above the highest Protective Marking permitted for the system, then the call should be terminated immediately ;

e. When using a system cleared to handle protectively marked information, callers should ensure they are familiar with any specific "secure mode indication" such as a handset indicator light or audio tone injection used by that particular system. Special care must be taken with those Legacy systems that use the now deprecated approach of audio tone injection, as differing MOD systems use these for diametrically opposite purposes.

1806. Where databases mapping telephone numbers to users or posts are present, the inference of the Data Protection Act is that the information will have to be protected as if it were Protectively Marked at least RESTRICTED, and should be specifically addressed in SPD which must be approved by the Accreditor(s).

Terminal Apparatus

1807. Only approved MOD owned apparatus is to be connected to telephone extensions (including ISDN ports) of an MOD telephone exchange, and it should be noted that this includes modems. Approval must be given by the IDA. The connection of non-approved apparatus to any exchange will be treated as a serious breach of security and will result in confiscation of the apparatus.

Voice Recording Services

1808. Voice messages can be recorded on either an answerphone connected to a telephone extension, or on a VoiceMail service attached to the telephone network, and there are differing security considerations for each case as given below.

1809. Although the sensitivity of information in any incoming message left on an answer-phone is the responsibility of the originator, the owner of each answer-phone or voicemail box user is to be responsible for regularly checking and clearing incoming messages, as there is some risk that individually UNCLASSIFIED messages could be collated to reveal sensitive information.

1810. **Answerphones** Where answer-phones are provided, irrespective of the network to which they are connected, they are not to be used to record protectively

marked messages. To this end, all callers who might leave a message are to be reminded of this rule by suitable words, such as :

> "This is the Answer-phone for Extension 1234. Please leave an UNCLASSIFIED message after the tone."

1811. **VoiceMail** There are inherent security risks in the use of voicemail systems. Voicemail is not to be used to record protectively marked messages. To this end, all callers who might leave a message are to be reminded of this rule by suitable words, such as

> "This is the voicemail-box for Extension 1234. Please leave an UNCLASSIFIED message after the tone."

1812. Voice Mailbox contents are liable to monitoring by the System Operating Authority (SOA).

1813. The PIN/Password for the mailbox should be changed by the user from the default to one that is not linked to person, post or office number.

1814. Facilities for the use of remote interrogation of mailboxes should not offer “backdoors” into other parts of the telephone system. Any evidence of possible malicious abuse of the system must be reported to Sector Security Staffs.

1815. Where SPD is raised in respect of a telephone exchange, the presence of a voicemail facility is to be reflected. If appropriate, this should be actioned retrospectively and the SPD should then be referred to the Accreditor.

Cordless Telephones

1816. Analogue (CT1) cordless telephones will not be approved as terminal instruments on extensions connected to a MOD telephone exchange.

1817. Digital (DECT) cordless telephones will not normally be approved as terminal instruments on extensions connected to an MOD telephone exchange, but regulations for their specific approval are contained at Annex B.

Mobile (Portable) Telephones

1818. Portable telephones present particular hazards to communications security. Detailed regulations for the use of portable telephones are shown at Annex C.

Voice Over Ip

1819. The Internet Protocol (IP) allows for various types of information, including

encapsulated Voice, to be carried over publicly accessible networks (PAN). The Protective Marking restrictions applicable to the PAN bearer will apply to the Voice being carried over that bearer**. For the Internet, this will mean that a limit of UNCLASSIFIED must be applied.**

Pagers

1820. Any information sent to a pager, or to the similar "SMS" capability of a mobile phone, should be UNCLASSIFIED only, and will be liable to mobile / portable telephone regulations if capable of transmit as well as receive operation.

Counter Eavesdropping

1821. Guidance on both the threat from audio-eavesdropping and on the required protective security measures is given **Chapter 27**.

1822. When considering the Protective Marking of any telephone call, it should always be remembered that there may be an indirect threat of additional information from "overhearing" of background audio content, which can include audio output from a computer, and keyboard and printer 'chatter'.

Compliance

1823. Compliance checks, including routine ComSec monitoring for transmission violations, may be carried out against all MOD telephony systems in accordance with **Chapter 12**.

Incident Handling

1824. Any security incidents affecting telephony systems must be handled in accordance with the regulations relevant to the installation, and a report raised to the Joint Security Co-ordination Centre (JSyCC), through the appropriate Monitoring and Reporting Centre (MRC) where applicable, in accordance with **Chapter 11**.

This page intentionally left blank.

ANNEX A TO CHAPTER 18

ACCREDITATION OF TELEPHONE EXCHANGES TO SECRET

1. The generic advice contained within this Annex has been withdrawn in the light of the availability of catalogue services from Defence Communication Service Agency (DCSA):

a. The Defence Fixed Telecommunications Service's (DFTS) Secure Speech Service (SSS) which will provide a network approved for SECRET across most sites served by MOD fixed telephony ;

b. Encrypting handset equipments approved to High Grade (HG) standard, as laid down at **Chapter 22**.

2. If any requirements are identified that do not appear to be able to be satisfied by either of these catalogue services, any telephone switch Accreditation in the variant solution must be sought directly from InfoSy(Tech). DCSA Infosec 3 (Copenacre (01225-81-) 3073) should contacted beforehand for details of the current solution approved for SSS, which will normally be the only solution acceptable in such cases.

This page intentionally left blank.

ANNEX B TO CHAPTER 18

CORDLESS TELEPHONES

Equipments

1. Cordless telephones, which include the analogue (CT1/CT2) and digital (CT3/DECT) technologies, rely on a radio link for part of any connection, and present specific security issues.

2. The use of analogue cordless telephones is prohibited for connection to any MOD telephone exchange.

3. This Annex addresses the Risks and Countermeasures relevant to the connection of Digital cordless telephones to MOD telephone exchanges.

The Threat Vulnerability and Risk

4. From events highlighted in national press and other sources there is evidence of persons wishing to gain access to telephone conversations and exploit the results of those interceptions.

5. Conversations made over analogue cordless telephones are easy to intercept and record. Digital technology provides a measure of protection by commercial encryption over the air interface, and has been approved for TranSec purposes only for protection of RESTRICTED information within the UK mainland.

6. An additional concern is the RadSec risk that operation of cordless telephones presents to other equipments in the vicinity. For this reason the following countermeasures are required.

Applicability

5. These regulations apply equally to officially supplied, privately owned and contractor owned cordless telephones when carried on MOD or service property, or being used for Official purposes.

Countermeasures

6. Specific precautions, and operating limitations, are required to minimise the risk of compromise of information by use of cordless telephones.

a. As a general principle, the use of cordless telephones is prohibited within MOD establishments and buildings ;

b. Cordless telephones are **specifically** prohibited from being used in buildings where protectively marked information is electronically stored, processed or forwarded, or in any other area so designated by the CIDA. Cordless telephones must be **switched completely off** (i.e. not left in "standby" mode) when entering such areas. Particular care is to be taken that if officially approved instruments are placed "on charge" within such an area that they do not inadvertently switch to the "on" or "stand-by" mode.

c. Cordless telephones are not to be taken into any room specially designated for secure conferences or a room/area where special technical security measures have been taken. Arrangements must be made by the Conference Security Officer (CSyO) or officers in charge of technically secure rooms to hold the instruments in safe custody in a location outside the secure facility.

d. Where a requirement is identified for the use of digital cordless telephones within the perimeter of an MOD site or establishment, the Commanding Officer or Head of Establishment must consult the appropriate Coordinating Installation Design Authority (CIDA) before designating either "Black" Zones within the site where the use of cordless telephones may be permitted, or alternatively "Red" Zones where cordless are prohibited, thereby allowing general use elsewhere within a site or establishment

e. Site and building specific regulations relating to the use of mobile telephones **must be prominently displayed** :

(i) At the entrance to any area where the use of mobile telephones is prohibited ;

(ii) At the entrance to any area where the carriage of mobile phones is prohibited ;

(iii) At the perimeter(s) of any designated Black Zones.

Additional Considerations

9. Cordless telephones should not be used in places denoted as "Hazardous Areas" or other areas where the use of such apparatus is prohibited under Health and Safety regulations. It should be noted that electronic equipments compliant with Civil EMC standards are not guaranteed to be immune from Radio Frequency Interference (RFI) from cordless telephones (e.g. DECT handsets) operated within 1m of the equipment in question.

ANNEX C TO

CHAPTER 18

MOBILE (PORTABLE) TELEPHONES

Overview

1. Mobile (portable) telephones, which include the major cellular telephone networks (BT Cellnet, One2One, Orange and Vodafone etc.) rely on a radio link for the whole or part of any connection. They may be hand carried devices or instruments forming part of an installation in a vehicle. In this Annex the term mobile telephone is used to cover all such devices.

2. The mobile telephone industry is a fast evolving area of technology, and is subject to a wide range of acronyms. **Appendix 1** provides a summary of the terminology and technologies that may be encountered in this area, as there may be some variation in the terms used by suppliers to that specified in this **Annex**.

Summary of Security Requirement

3. At present the only mobile telephone standards approved for use with Protectively Marked Official information are those conforming to the Global System for Mobiles (GSM900 / GSM1800 / GSM1900) standards, which are the dominant form of mobile (portable) telephones used within the MOD. The following table summarises the general usage restrictions, with more detailed advice later in this Annex :

	Within UK Mainland	**Anywhere Else**
Circuit Switched Voice Calls	RESTRICTED	UNCLASSIFIED
Circuit Switched Data Calls to MOD CIS accredited to RESTRICTED	RESTRICTED	Not normally permitted
Circuit Switched Data Calls to UNCLASSIFIED systems including the Internet	UNCLASSIFIED	
Use of GPRS service (*"2.5G" phones only*)	UNCLASSIFIED	
Use of SMS service	UNCLASSIFIED	

4. In addition to the constraints on the type of material that may be transmitted over mobiles telephones, there are constraints on their use on MOD property, as laid down later in this Annex.

5. Terrestrial Trunked Radio (Tetra), and other related Private Mobile Radio (PMR) technologies, which may be used in a manner analogous to mobile phones, are addressed in **Chapter 26**.

The Threat Vulnerability and Risk

6. From events highlighted in national press and other sources there is evidence of persons wishing to gain access to mobile telephone conversations and exploit the results of those interceptions. Conversations made over analogue mobile telephones, are particularly easy to intercept and record.

7. Cellular telephones, especially vehicle mounted apparatus, are accessible over a fairly wide area, and present considerable risks to users unless their conversations are encrypted by approved means. The emergent technologies based on Low Earth Orbit (LEO) satellite mobile access inherently broadcast their information over an even wider area.

8. Cellular telephones intermittently transmit to maintain communication with a base station even though not being used for speech at the time, they therefore present a further TEMPEST hazard when in close proximity to CIS; they could compromise any unencrypted information being processed.

9. Additionally products are now being which uses these intermittent transmissions to localise mobile telephony devices, and in some case offered in conjunction with Global Positioning System (GPS) technology which gives a high degree of precision. This may be a risk in Operational cases where the user(s)'s whereabouts are intended to be concealed.

10. Some models of mobile phones have an ability to be remotely activated even when notionally switched off, and can inadvertently or deliberately therefore act as an eavesdropping device.

Applicability

11. These regulations apply equally to officially supplied, privately owned and contractor owned mobile telephones when carried on MOD or service property, or being used for Official purposes, and for its use for Voice purposes.

12. When a mobile telephone is to be used for purposes other than Voice, additional considerations must be taken into account:

a. Fax purposes : the regulations covering Facsimile as laid down at **Chapter 19** must be followed in addition to the measures laid down in this Annex ;

b. Data purposes (including WAP): in addition to the measures laid down in this Annex, the constraints relevant to both the connecting bearer (as laid down at **Chapter 22** and **Chapter 24**), and to any end system (e.g. **Chapter 10** for the Internet, or in the system's SSP) must also be followed.

13. Any modes of use not covered in the above paragraphs should be assumed to only be approved for UNCLASSIFIED purposes, and InfoSy(Tech) should be consulted for specific guidance.

Countermeasures

14. Specific precautions, and operating limitations, are required to minimise the risk of compromise of information by use of mobile telephones.

15. Device dependant considerations :

a. Legacy analogue (1G) mobile telephones are only to be used for UNCLASSIFIED speech. It is the responsibility of the analogue user to ensure that other parties are aware of this limitation ;

b. GSM900 / GSM1800 mobile telephones when being operated within mainland UK are approved for voice telephone calls up to and including RESTRICTED without additional countermeasures.

c. Where there is any requirement for the use of GSM technology (including such technologies embedded in notebook computers or PDAs) to be used in Circuit Switched Data (CSD) or General Packet Radio Service (GPRS) modes for the passage of official information, specific approval must be obtained in advance from the relevant PSyA or the DSSO. Any devices enabled for GPRS/EGPRS services must be configured to allow the user to control the activation of the link ;

d. The Signalling System 7 (SS7.05) Short Message Service (SMS) is limited to UNCLASSIFIED use only ;

e. When any mobile phone is being operated outside of mainland UK ("roaming"), all calls involving this device are limited to UNCLASSIFIED only, and it is the responsibility of the roaming user to ensure that other parties are aware of this limitation ;

f. LEO satellite mobile phones are only to be used for UNCLASSIFIED speech. It is the responsibility of the LEO user to ensure that other parties are aware of this limitation ;

g. Dual or multi mode (e.g. GSM cellular / DECT cordless and GSM cellular / LEO satellite mobile) devices are to be used in accordance with the most prescriptive requirements;

h. Any other classes of device (including all 3G services) are to be operated at UNCLASSIFIED only until specific guidance has been obtained from InfoSy(Tech) via the security chain of command.

16. It should be noted that the User Identification details (including home country and network) for both analogue and digital mobile phones are passed in clear, and this may provide a way for either network operators or interceptors to track movements of, for instance, a VIP.

17. Site dependent considerations :

a. As a general principle, the use of Mobile telephones is prohibited within MOD establishments and buildings, and mobile telephones must be switched completely off (i.e. not left in any “standby” or quiescent “always on” mode). Particular care is to be taken that if terminal equipments (e.g. handsets) are placed “on charge” within MOD sites that they do not inadvertently switch to the "on" or "stand-by" mode ;

b. Mobile telephones are not to be taken into any room specially designated for secure conferences or a room/area where special technical security measures have been taken.

Arrangements must be made by the Conference Security Officer (CSyO) or officers in charge of technically secure rooms to hold the instruments in safe custody in a location outside the secure facility.

c. Where a requirement is identified for the use of mobile telephones within the perimeter of an MOD site or establishment, the Commanding Officer or Head of Establishment must consult the appropriate Coordinating Installation Design Authority (CIDA) before designating either “Black” Zones within the site where the use of mobile telephones may be permitted, or alternatively “Red” Zones where mobiles are prohibited, thereby allowing general use elsewhere within a site or establishment

d. Site and building specific regulations relating to the use of mobile telephones **must be prominently displayed** :

(i) At the entrance to any area where the use of mobile telephones is prohibited ;

(ii) At the entrance to any area where the carriage of mobile phones is prohibited ;

(iii) At the perimeter(s) of any designated Black Zones.

Additional Considerations

18. Mobile telephones should not be used in places denoted as "Hazardous Areas" or other areas where the use of such apparatus is prohibited under Health and

Safety regulations. It should be noted that electronic equipments compliant with Civil EMC standards are not guaranteed to be immune from Radio Frequency Interference (RFI) from mobile telephones (e.g. GSM Class 4 or PCN Class 1 handsets) if the impinging electromagnetic field exceed $2Vm^{-1}$, which is the extreme case operated within 3m of the equipment in question.

19. Users of mobile telephones are to comply with any instructions or regulations appertaining to their use at any establishment or organisation which they may be visiting.

APPENDIX 1 TO ANNEX C TO CHAPTER 18

MOBILE TELEPHONE TAXONOMY

The following table summarises the current and predicted terminology and technologies in the mobile telephone industry. It will be noted that some terms (e.g. PCS) are used to describe multiple differing technologies.

Generation	Service	Standards	Applicability	Notes and Additional Network Facilities
1G	Total Access Communications Service (TACS) and Enhanced Total Access Communications Service	FDMA	UK / Europe	N/A
	Advanced Mobile Phone Service (AMPS)		USA / CAN	
	Nordic Mobile Telephony (NMT)		Scandinavia	
2G	Digital-AMPS (D-AMPS)	TDMA IS-54	USA / CAN	*Interim standard with mix of analogue and digital: superceded by IS-136*
	Global Standard for Mobiles (GSM) at 900Mhz (GSM900) and 1800Mhz as Personal Communications Service (PCS1800 / GSM1800)	200kHz 8 timeslot TDMA	Worldwide	• Short Message Service (SMS) ≤160 bytes • Circuit Switched Data (CSD) 9.6-14.4 kb/s
	GSM at 1900Mhz (GSM1900 / PCS1900)		USA / CAN	
	United States Digital Cellular (USDC) or Digital PCS	3 timeslot TDMA IS-136 TIA/EIA-136	North / South America	
	CdmaOne AMPS or Digital PCS	CMDA IS-95	USA / CAN	
	Personal Digital Cellular (PDC) or Personal Handyphone System (PHS)		Japan	

Generation	Service Name(s)	Standards	Applicability	Additional Network Facilities
2.5G Phase 1	2.5G or GSM2001	200kHz 8 timeslot TDMA with Gaussian Minimum Shift Keying (GMSK)	All GSM markets	• Short Message Service (SMS) ≤160 bytes • High Speed Circuit Switched Data (HSCSD) at n*14.4 kb/s (1≤n≤4) • General Packet Radio Service (GPRS) at n*13.2 kb/s (2≤n≤8) where n = a + b a = "up" slots b = "down" slots
2.5G Phase 2	Enhanced Data rates for GSM Evolution (EDGE)	200kHz 8 timeslot TDMA with Eight Phase Shift Keying (8PSK)	All GSM markets	• Short Message Service (SMS) ≤160 bytes • Enhanced Circuit Switched Data (ECSD) n*14.4 kb/s (1≤n≤8) • Enhanced General Packet Radio Service (EGPRS) ≤384 kb/s
3G	International Mobile Telephone 2000 (IMT-2000), formerly Universal Mobile Telephone System (UMTS)	Wideband CDMA (WCMDA) ITU M.687	Worldwide	• Local area data ≤2Mb/s • Wide area data ≤384 kb/s • cdma2000 narrowband mode • Time Division Duplex (TDD) mode

This page intentionally left blank.

ANNEX D TO CHAPTER 18

VOICEMAIL

1. Voicemail is not to be used to record protectively marked messages. To this end, all callers who might leave a message are to be reminded of this rule by suitable words, such as "This is the voicemail-box for extension 1234. Please leave an UNCLASSIFIED message after the tone.".

2. Though the sensitivity of information in any incoming message is the responsibility of the originator, the owner of each voicemail-box is to be responsible for regularly checking incoming messages and flushing them out where necessary. Note that there is some risk that individually UNCLASSIFIED messages could be collated to reveal sensitive information.

3. Mailbox contents should be periodically monitored and any abuse should be dealt with promptly.

4. The time allowed for recording incoming messages is to be minimised.

5. If the system permits, the total amount of information on the voicemail system is to be kept to a minimum by some form of purge or ageing-off procedure.

6. The PIN/Password for the mailbox should be changed by the user from the default to one that is not linked to person, post or office number.

7. Facilities for the use of remote interrogation of mailboxes should not offer backdoors into other, possibly sensitive, parts of the telephone system. Any evidence of possible malicious abuse of the system must be reported through the security chain of command.

8. Where Security Policy Documentation (SPD) is raised in respect of a telephone exchange, the presence of a voicemail facility is to be reflected. If appropriate, this should be actioned retrospectively and the SPD should then be referred to the accreditor.

This page intentionally left blank.

FACSIMILE SECURITY

CHAPTER 19

FACSIMILE SECURITY

Introduction

1901. Facsimile equipment is provided for the transmission of documents and signal messages over either dedicated (point to point) or telephone (dial up) lines such as those provided by Government or Service telephone systems, British Telecom, Mercury or other commercial organizations. Because of the inherent dangers of passing Government information accidentally or intentionally to unauthorised recipients via facsimile, it is necessary to ensure that the use of such equipment is strictly controlled.

1902. If it is necessary to use a facsimile machine for copying, it must also comply with the copier rules laid down in **Volume 1**, and must not be used to copy material of a higher protective marking than that authorized for transmission from the terminal.

1903. When planning the procurement, installation, re-siting or removal of any facsimile machine, irrespective of whether or not it is intended to either transmit or receive protectively marked material, the CIDA and security chain of command must be consulted so that security risks can be assessed and countermeasures considered.

1904. Additional records may be required for financial audit.

Applicability

1905. This chapter gives the basic instructions that are applicable to all dedicated facsimile devices i.e. insecure and secure facsimile and insecure and secure DISKFAX. The instructions are based on insecure facsimile machines and additional information on the extra rules that apply to secure facsimile and DISKFAX are at Annexes A and B respectively.

1906. Additional technologies now exist which are capable of carrying out the same functions as dedicated facsimile machines, including :

a. FAX modem cards for personal computers (PCs) ;

b. FAX servers for connection to computer networks ;

c. FAX mailboxes provided by Public Telephony Operators ;

d. FAX service provided on the Internet.

1907. In general the same principles as laid down in this chapter should be used for these additional technologies, but the technology specific paragraphs in this Chapter must also be complied with. Any technologies not specifically mentioned within this Chapter can be assumed to not be currently approved for MOD use, and any requirement for use of such technologies should therefore be referred to InfoSy(Tech) for direction.

Administration And Control

1908. Each facsimile and DISKFAX terminal must have a nominated Controller as follows:-

a. **Insecure.** Any Service Officer, any Senior NCO, or Civil Servant at Band E1 (or equivalent) or above ;

b. **Secure.** Any Service Officer, or Civil Servant at Band D (or equivalent) or above.

1909. He/she is responsible for overseeing its day to day operation. A Deputy Controller is to be nominated to cover periods when the Controller is absent. The Controller is to be appointed before the facsimile terminal is installed, to assist in the planning and development of working practices.

Security Policy Documentation

1910. Full Security Policy Documentation (SPD) is not required for individual facsimile installations, and Security Operating Procedures (SyOPs) produced in accordance with this Chapter will therefore suffice.

1911. The nominated Controller must produce written SyOPs for each secure and insecure terminal under his/her control. These SyOPs must reflect the requirements of this document and be approved by the relevant security authority before a terminal is first used. The SyOPs must be brought to the attention of users. A suggested format for SyOPs is shown at Annex C for facsimile and Annex D for DISKFAX.

1912. The Controller is to maintain a list of persons authorized to use the terminal. The Controller or an authorized Deputy is responsible for ensuring that each transmission has been properly authorized and that the terminal is suitable for the transmission in accordance with para 1818 and paras 1815 - 1816 below.

Physical Security

1913. **General.** Facsimile equipment should be located in a room where general access to the machine is denied but in which at least one person, ie the Controller or his/her Deputy is on duty.

1914. Plain paper facsimile machines use a process similar to that of a photocopier/laser printer to produce the message image. The process gives rise to an extra security problem. Detailed below is the specific measure to be taken; before

turning the machine off at close of play, ensure that a test print is made to clear the facsimile's memory. If a memory capability is available, PIN code protection must be enabled.

1915. When an office is unattended, the facsimile machine must be immobilized to prevent unauthorized use. This can be achieved either by:

a. Disabling the transmit portion of the facsimile on machines where this facility is provided typically by a key switch,

or

b. Locking the access door to the room where the facsimile is installed,

1916. Where unattended out of hours working in the `receive mode only' is required, or if the above cannot be achieved :

either

a. The equipment is in a designated secure area or locked room.

i. Appropriate security management controls are applied.

ii. No unauthorized viewing is possible.

or

b. If a memory system is in use, the PIN code is enabled.

1917. A weekly transmission journal must be retained in accordance with the requirements set out in the SyOPs.

Document Security

1918. All pages of a document to be transmitted by the facsimile must be clearly marked with the protective marking, top and bottom, situated centrally and the page number.

Transmission Security

1919. **General.** Depending on the geographical location, terminals are only authorised to transmit or receive certain levels of protectively marked information, as detailed below:

a. Between terminals located within mainland UK. These may be used to transmit information which is UNCLASSIFIED or RESTRICTED. NATO UNCLASSIFIED information may also be passed but not NATO RESTRICTED. Before transmitting any material bearing a privacy marking, the Controller/Supervisor of the receiving terminal/machine is to be contacted to

ensure that the facilities for handling such material are in place. No `Special Handling' information may be passed.

b. From, to or between any terminal located outside mainland UK - including Northern Ireland. Only UNCLASSIFIED or NATO UNCLASSIFIED information may be passed.

c. Facsimile transmissions of RESTRICTED information to and from Northern Ireland must always be by secure means.

1920. **Warning Notices.** Each facsimile terminal is to bear a notice indicating the highest protective marking of material that can be passed over the system, in accordance with the following:

a. For insecure terminals in mainland UK the notice is to read:

`THE TRANSMISSION OF INFORMATION PROTECTIVELY MARKED HIGHER THAN UK RESTRICTED, NATO UNCLASSIFIED OR CONTAINING A SPECIAL HANDLING CAVEAT IS FORBIDDEN. UNCLASSIFIED INFORMATION ONLY CAN BE TRANSMITTED TO NORTHERN IRELAND AND OVERSEAS'.

`Violations of Transmission Security are to be reported immediately to the Controlling/Supervising Officer or Establishment Security Officer'.

Signed:..... Controlling Officer:..... Date:.....

b. For all other insecure terminals overseas or in Northern Ireland the notice is to read:

`UNCLASSIFIED DATA ONLY. NOT TO BE USED FOR TRANSMITTING PROTECTIVELY MARKED, RESTRICTIVE CAVEAT OR SPECIAL HANDLING DOCUMENTS'.

`Violations of Transmission Security are to be reported immediately to the Controlling/Supervising Officer Establishment Security Officer'.

Signed:..... Controlling Officer:..... Date:.....

Facsimile Transmission Proforma

1921. Each document to be transmitted by an insecure facsimile must be accompanied by a `Facsimile Transmission Cover Sheet' (F Sigs 927) (which must be the first page) or a "FAX Post It" note or a rubber stamp may be used. The stamp must allow details of the sender, intended recipient, sender's telephone number and number of pages sent to be entered. Each document must also be correctly authorized (see para 1818). [Note: If the message is to sent via a commcen then the F Sigs 927 form must be used.]

1922. Where the facsimile is to be transmitted to an addressee other than a part of MOD, Other UK Government Department, or Allies, the F Sigs 927 is to be used, with the following additional disclaimer included in the "Messages" box:

> "The information contained in this facsimile and any subsequent correspondence is private and is intended solely for the recipient, for those other than the recipient any disclosure, copying, distribution, taken or omitted to be taken in reliance on such information is prohibited and may be unlawful."

Authority for Facsimile Transmission

1923. The authorizing Officer must satisfy himself that the document to be transmitted bears the correct protective marking. Any cases of doubt are to be referred back to the sponsor/originator of the document. Facsimile transmissions may be authorized as follows:

Insecure

a. **Unclassified or RESTRICTED.** Any Service Officer, any Senior NCO, or Civil Servant at Band E1 (or equivalent) or above

Secure

b. **CONFIDENTIAL.** Normally, an Officer not lower in rank than Lieutenant RN, Captain, Flight Lieutenant, Civil Service Band D or the equivalent.

c. **SECRET.** Normally, an Officer, not lower in rank than Lieutenant Commander, Major, Squadron Leader, Civil Service Band C2 or the equivalent.

d. **TOP SECRET.** Normally, an Officer not lower in rank than Commander RN, Lt Colonel, Wing Commander, Civil Service Band C1 or equivalent or by a Resident Clerk or a Private Secretary to a member of a Council or Board.

1924. Exceptionally, HOEs/Cos/Directors may delegate authorization for facsimile transmission to those persons within their organisation whom they deem to be sufficiently experienced and reliable to ensure that adequate control of security procedures is maintained.

Transmission Procedures

1925. When using dial up facilities, care must be taken by the operator that the correct number has been dialled before transmitting any facsimile material. If it is discovered that a facsimile message has gone to an incorrect terminal, due to faulty dialling or misrouting, the actions set out in paras 1824-1826 below are to be followed.

1926. The most common reason for the misdirection is the incorrect use of Public Switched Telephone Network (PSTN) dialling codes, often and sometimes inaccurately referred to as "outside line" or "BT" (British Telecom) codes. Users are reminded that before they dial any PSTN code they must normally precede it with either a 0 or 9 (dependent upon telephone exchange) to connect the line. PSTN should not be used as the first choice for connection but as a last resort. Users of insecure facsimiles who are using stored PSTN numbers are to check that they have preceded the code with the correct access digit described.

1927. The order of precedence to be used when making facsimile transmissions is as follows:

a. Use the Defence Fixed Telecommunications Service (DFTS), the use of which does not incur charges from Public Telephony Operators (PTO) ;

b. Use the Government Telephone Network (GTN) which not only provides access to MOD establishments but also to other Government Departments. There is a charge for this service but it is less than the equivalent call made through PTOs ;

c. Use the Government Out of Area Lines Service (GOALS) which is a feature of the GTS which allows trunk (long distance) calls to be made at local call charge rates ;

d. Use the PSTN.

1928. Most facsimile machines allow users to insert both the telephone number and a terminal identifier (normally the branch name) of the facsimile machine. Both of these items are displayed on every page transmitted and also they are shown on the display panel of facsimile machine trying to transmit to it. It is recommended that both these options are used as they provide a simple method of checking that the correct connection has been prior to transmission.

Transmission Security Violations

1929. Transmission security violations occur when any protectively marked information is passed over communication circuits, including facsimile, not approved for that particular protective marking; this includes the partial transmission of a protectively marked document.

1930. It is essential to report any violation of transmission security at the earliest opportunity to reduce the effects of the compromise of the information. Under no circumstances should attempts be made to conceal a transmission violation.

1931. When a facsimile document is discovered to have suffered a transmission security violation, the Controller of the facsimile terminal must inform the originator of the document, by other means than FAX, and then in consultation with the relevant Principal Security Advisor (PSyA) :

a. Notify immediately those addressees who need to know that the document has been compromised. This to be done by other means than FAX ;

b. Determine and initiate action to minimize the effects of the compromise, if necessary in consultation with higher authority ;

c. Follow the incident reporting requirements of **Chapter 11** ;

d. Take steps to recover a misdirected document.

Repair, Maintenance and Disposal

1932. Stored numbers should be erased from memory before the equipment is sent for repair or disposal.

1933. Some equipments also have a volatile memory acting as a buffer store for data transmitted or received. This buffer store is normally cleared when the machine is switched off but for added security an UNCLASSIFIED A4 size paper with a computer picture such as a computer test pattern or similar document followed by a blank sheet of paper should be fed through the machine before the equipment is sent away for repair or disposal.

1934. Maintenance on site should undertaken by security cleared UK nationals who are to be supervised at all times. Engineers who are not security cleared are to be escorted and supervised at all times. A log is to be maintained of all repairs.

Remote Diagnostics

1935. Remote diagnostics where fitted are to be permanently disabled.

Use of Facsimile for Signal Messages

1936. Facsimile Systems are not part of the Defence Communications Network (DCN) and do not support the integrity and accounting functionality provided by ACP 127 networks. However, facsimile offers a means of clearing formal signal messages. Policy is provided here primarily to provide guidance for COMMCEN personnel and staff, to specify responsibilities and to define a minimum set of common procedures throughout Defence. Details are provided in **Chapter 23**.

Fax Modems

1937. In addition to complying with the requirements for facsimile machines laid down in this Chapter, the installation of a “FAX modem” in any personal computer will require the adaptation of the generic Security Policy Documentation (SPD) for such

systems laid down at **Chapter 1** to accommodate the changed configuration, and will thus require specific Accreditation by the PSyA or DSSO rather than simple Registration.

1938. A common feature of FAX modems is the ability to send and receive facsimile (fax) messages to and from similarly equipped computers or ordinary fax machines, in addition to being able to communicate with other modem-equipped computers or computer networks. Switching between these two modes of operation is usually controlled by software. Despite their apparent advantages, fax/modems represent a significant threat to system security because their usefulness depends largely on continuous dial-in access and they are therefore especially vulnerable to hacking.

Fax Servers

1939. In addition to complying with the requirements for facsimile machines laid down in this Chapter, the presence of the "FAX server" on the network must be factored into the Assurance Requirement assessment for the network to be carried out in accordance with **Annex A to Chapter 14**. If there is any intention to directly or indirectly connect the FAX server to the PSTN, then the Attacker Populace will by definition be greater than 5,000 uncleared persons.

Fax / Internet Mailboxes

1940. In addition to complying with the requirements for facsimile machines laid down in this Chapter, "FAX mailboxes" provided by Public Telephony Operators, and Internet based FAX services utilise "store and forward" technology without any assertion being possible as to the protection of data either in transmission or in storage. It is therefore not permitted to use such service for other than the transmission of UNCLASSIFIED material, and where a telephone number for either a PTO or Internet FAX mailbox is published, it must be clearly shown that it can only be used for the receipt of UNCLASSIFIED material only.

ANNEX A TO

CHAPTER 19

ADDITIONAL INSTRUCTIONS FOR THE USE OF SECURE FACSIMILE EQUIPMENT

Introduction

1. A secure facsimile is defined as a facsimile terminal connected to a Government approved High Grade (HG) cryptographic device.

2. When a secure facsimile terminal is required the appropriate communications and security authorities must be consulted and their approval obtained before the equipment is procured and installed. Normally, secure facsimile systems are approved to carry information protectively marked SECRET and below. Where a user has a requirement to pass a higher protective marking or caveated information, specific authority must be sought from Defence ComSec Operating Authority at DCSA on a case by case basis. Secure facsimiles are not intended to replace the courier mail system or signal system and the use of these machines should only be considered when there is an urgent need to pass copies of protectively marked documents quickly.

3. Secure facsimile installations must conform to physical and communication security criteria. No alterations are to be made to a secure facsimile installation without the approval of the IDA and relevant PSyA.

Physical Security

4. The cryptographic equipment, keying material and authentication systems are to be protected in accordance with National Cryptographic Instructions. Whilst these instructions apply to the cryptographic equipment, the same rules for unattended operation as in Paras 1809 - 1813 apply to the security of the facsimile equipment and the material received. In addition all keys associated with the facsimile equipment are to be removed from locks and stored in an appropriate security container. A register of these keys is to be maintained.

Document Security

5. All pages of a document to be transmitted by the facsimile must be clearly marked with the protective marking, top and bottom, situated centrally and the page number.

6. Transmission and receipt of documents protectively marked SECRET and above is to be recorded in a Protectively Marked Document Register (MOD F102). Depending on the volume of faxes, Controllers may need to maintain two MOD F102s, one for outgoing messages and one for incoming messages. Recording of outgoing and incoming messages at a COMMCEN may be carried out using an approved communications register.

Transmission Security

7. Information protectively marked up to and including SECRET may only be transmitted between terminals which have been certified `secure' by the relevant COMSEC authority (except for RESTRICTED information within mainland UK). Each terminal must display a certificate to this effect (see para 10 below).

8. **TOP SECRET and Special Handling.** Information protectively marked TOP SECRET or bearing a security caveat that requires special handling may only be sent from and to specifically approved facsimile terminals. Each transmission must be authenticated (using an approved authentication system) as prescribed by the Defence ComSec Operating Authority; unofficial or locally devised authentication systems are forbidden.

9. Where a document protectively marked TOP SECRET or requiring special handling is to be transmitted over the secure facsimile, prior arrangements must be made by telephone to ensure that the intended recipient of the document is present at the receiving terminal. The transmission proformae must bear the following marking:

> "Exclusive For" Name or Appointment of the recipient or the person nominated to receive such documents on his behalf.

Where a secure facsimile machine serves more than one department within a HQ or Unit, the Controlling Officer must keep a list of nominated personnel for each Dept/Unit.

10. **Warning Notices.** Each facsimile terminal is to bear a notice indicating the highest protective marking of material that can be passed over the system, in accordance with the following:

> For secure terminals the notice is to read:

`NOT TO BE USED FOR TRANSMITTING DOCUMENTS PROTECTIVELY MARKED HIGHER THAN..... (protective marking for which the system has been approved). FOR CAVEATED OR TS INFORMATION FIRST LOAD THE APPROPRIATE KEY MATERIAL AND AUTHENTICATE USING MATERIAL HELD BY THE CONTROLLING OFFICER.

`Violations of Transmission Security are to be reported immediately to the Controlling/Supervising Officer, Branch Security Officer or Unit Security Officer'.

Signed:..... Controlling Officer:..... Date:.....

Signed:..... COMSEC Authority:..... Date:.....

Facsimile Transmission Proforma

11. Each document to be transmitted by a secure facsimile must be accompanied by a `Facsimile Transmission Cover Sheet' (F Sigs 927) and be correctly authorized (see para 27). For transmissions protectively marked SECRET or above or for documents bearing a Special Handling Caveat the following rules are to be implemented:

a. A form `in-lieu' of MOD Form 24 is to be transmitted as the last page of any document.

b. Where a secure facsimile is serving a number of departments in a large HQ or Units within an Establishment, prior arrangements are to be made with the receiving Controlling Officer regarding the copying and distribution of documents before the transmission is allowed.

c. The distribution of the transmitted facsimile is to be shown on the transmission proforma including copy numbers of the documents.

d. Copy numbers are also to be marked on the front page of the document NOT the transmission proforma in the following manner.

"REPRODUCTION COPY NO OF COPIES ."

12. The Facsimile Transmission Proforma, when used, must be transmitted as the first page of any facsimile document.

13. After transmission, the facsimile transmission proforma is to be retained by the Controller for six months. Where the terminal generates a journal, the proforma are to

be checked against the journal and filed with the journal and will be subject to spot checks by security staffs.

Transmission Procedures

14. Before transmitting a document protectively marked TOP SECRET, or material requiring special handling, contact must be made with the distant terminal by telephone or telegraphic means to ensure that the receiving terminal is manned by a person authorized to receive the material. All TOP SECRET and special handling material must be authenticated. Instructions for authentication are provided with authentication tables. (If a dedicated point to point system is in use voice authentication will suffice.)

15. Unless specifically requested by the sender Unclassified, RESTRICTED or CONFIDENTIAL items need not be acknowledged; however, for all items or batch items protectively marked SECRET or above (and those CONFIDENTIAL, RESTRICTED and Unclassified items for which acknowledgement has been requested) the following applies:

a. Receipt is to be acknowledged by the addressee at the receiving terminal by telephone or facsimile at the end of the transmission.

b. When a document protectively marked SECRET or above is sent via facsimile, the originator should also send a form, in lieu or MOD F24, for signature by the recipient which is to be returned to the originator by normal means, ie post.

c. For all facsimile transmission protectively marked SECRET and above and for those documents with special handling caveats they must be entered in a MOD F102.

16. Aborted copies produced as a result of an equipment malfunction but containing eye readable protectively marked information are to be registered in a MOD F102 and destroyed in accordance with the appropriate destruction procedures.

Receipt Procedures

17. The following procedures for receipt are to be implemented:

a. In the case of the transmission proforma or alternatives that are received with a facsimile message for a document protectively marked CONFIDENTIAL or below, these are to form a receipt log which is to be retained for a period of six months.

b. The transmission proforma in respect of documents protectively marked SECRET and above or those carrying special handling markings are to be retained for a period of two years.

c. All material received is to be passed to the addressee. In the case of documents protectively marked SECRET or above or documents carrying special handling caveats, they are to be entered in the receiving MOD F102 and passed on signature to the addressee.

d. When prior arrangements have been made for the Controlling Officer at the receiving terminal to copy a document protectively marked SECRET or above or requiring special handling, the following rules are to be applied:

(1) Copies of the document must only be made on a machine cleared to copy such material and the photocopier log is to be annotated accordingly.

(2) Copies of the document are to be marked as in Paragraph 11d above by the Controlling Officer.

(3) All copies are to be entered into the incoming MOD F102 and passed to the addressees on signature.

Repair, Maintenance and Disposal

18. Maintenance on site for secure terminals is to be undertaken by security cleared UK nationals who are to be supervised at all times. A log is to be maintained of all repairs.

Secure Facsimile Over PATRON Extensions

19. **Background**.

a. MOD Common User Secure Facsimile (MOD CUSECFAX) is to be retained as the MOD core secure facsimile system. PATRON was designed as an interim secure speech system, and any use of the PATRON system as a bearer for facsimile transmissions is to be regarded as a concession.

b. Operational sponsor is defined as the nominated Sector appointment that represents the user, and will endorse (or not) any requirement for facsimile over PATRON (satisfying himself first that MOD CUSECFAX is not appropriate), and confirming that appropriate funding is available.

20. **Policy for Secure Facsimile over PATRON Extensions**. When endorsed by the sector MOD CUSECFAX and the sector PATRON operational sponsors, facsimile machines may be used on PATRON telephone extensions to transmit and receive protectively marked traffic up to and inclusive of TOP SECRET UK EYES (non-STRAP), provided the TEMPEST installation rules and the procedural rules are applied. It is stressed that requirements for facsimile over PATRON are only to be endorsed when MOD CUSECFAX is deemed as inappropriate.

21. **Endorsement by Sector MOD CUSECFAX Sponsor**. All applications for facsimile over PATRON (including re-siting and removal of existing systems) are to be endorsed by the relevant Sector MOD CUSECFAX sponsor (see list at paragraph 23 below).

22. **Rules and Procedures**. Where a case is approved for the use of facsimile over PATRON, rather than MOD CUSECFAX, particular attention is to be drawn to the following rules and procedures:

a. The facsimile equipment is to meet Group 3 and preferably STANAG 5000 standards.

b. The facsimile equipment is to use a PATRON approved telephone line. This will normally be a new PATRON extension specifically installed for the facsimile equipment.

c. The installation of the facsimile equipment is to be by an approved Coordinating Installation Design Authority or Installation Design Authority (CIDA/IDA), whichever is appropriate.

d. The facsimile installation (telephone and facsimile equipment) is to be prevented from making calls to non-PATRON extensions by technical measures such as number barring at the exchange and/or physical means such as fixing a cover over the dial key pad and allowing the subscriber to use pre-programmed memory buttons only.

e. External diagnostics are to be disabled and a regular 3 monthly check made to ensure that they remain disabled. Specific checks are to be made immediately following service or repair.

f. PATRON facsimile equipments are to be set to receive voice first (requiring physical intervention to switch to receive facsimile after authentication/voice recognition is complete) and are not to be operated in the unattended receive mode.

g. The caller is to be satisfied that a PATRON link has been established and that the recipient is authorised to receive the information, prior to any facsimile transmission.

h. All transmissions and receipts are to be recorded and acknowledged in accordance with current procedures for facsimile transmissions of protectively marked information.

23. **Sector MOD CUSECFAX Sponsor**. The overall Defence MOD CUSECFAX security authority is the Defence ComSec Operating Authority in DCSA. Sector MOD CUSECFAX sponsors (from whom prior endorsement of all PATRON facsimile installations is to be obtained) are as follows:

a. Navy - DCIS(N)

b. Army - DCIS(A)

c. RAF - DCIS(RAF)

d. All other units - DCSA

This page intentionally left blank.

ANNEX B TO

CHAPTER 19

ADDITIONAL INSTRUCTIONS FOR THE USE OF SECURE AND INSECURE DISKFAX DATA TRANSFER EQUIPMENT

Introduction

1. DISKFAX is the commercial name given to a device which enables the transfer of data stored on either 3.5 or 5.25 inch diskettes between similar equipment via "dial-up" telephone lines. Despite the name, it is a data transfer device and not a facsimile. There are two variants of DISKFAX, one fitted with a non-removable integral hard disk and the other with no hard disk facility. DISKFAX does not provide any security protection to the data either in storage or transmission and is considered to operate in DEDICATED mode.

2. When planning the procurement, installation, re-siting or removal of any DISKFAX machine, irrespective of whether or not it is intended to either transmit or receive protectively marked material, the appropriate communications and security authorities must be consulted so that security risks can be assessed and countermeasures considered.

Applicability

3. This Annex applies to all DISKFAX used within Defence and Defence Contractors for the transfer of official information and no departure from or variation to it is permitted unless prior authorization is obtained from the appropriate security authority.

4. **Constraints.** The following constraints apply:

   a. DISKFAX is only to be used for the transfer of official information.

   b. DISKFAX is only to be operated with another DISKFAX machine. It is NOT to be connected directly to a PC.

c. DISKFAX is only to be used with encryption devices approved by COMSEC authorities when encryption is required.

5. **Installation.** DISKFAX is to be installed as a stand-alone equipment connected to a telephone line via an approved telephone socket. Installation is to be in accordance with the instructions provided with the equipment and siting of the equipment is to be under the direction of the relevant Installation Design Authority (IDA). On installation the following items are to be programmed:

a. The Directorate/Branch/Unit name and the telephone number of the line to which connected.

b. An instruction to produce a log of **every** transmission.

Administration and Control

6. Branches operating, or intending to operate, DISKFAX equipment are to notify their local security staffs who are to ensure that security instructions are produced and are available to all users of the equipment. The security staffs is to ensure that any DISKFAX equipment within his area of responsibility is operated strictly in accordance with the laid down security procedures and is to ensure that a DISKFAX Controller of at least Lieutenant(RN), Captain, Flight Lieutenant, Civil Service Band D or equivalent is appointed for the day-to-day supervision of the equipment. A deputy should also be appointed. The security staffs are to ensure that the appointed officers are aware of their security responsibilities relating to the equipment.

Physical Security

7. The equipment is to be switched off and secured whenever the office or other area in which it is located is to be unattended for any period of time exceeding the normal 30-minute rule. When unattended all removable magnetic media (e.g. Floppy Disks) must be securely stored in a container or secure room appropriate to the highest protective marking of material ever stored or transmitted on the machine, and of at least adequate level for protecting RESTRICTED information. If a DISKFAX with fixed hard disc is used, the equipment must be treated in the same manner as removable media i.e. it must be securely stored as laid down above.

8. Where none of the above can be achieved, the DISKFAX machine must be disconnected and stored in a secure cabinet. In special cases, the security and communications authorities may authorize unattended out of hours working in the `receive mode only' provided that:

a. The equipment is in a designated secure area or locked room.

b. Appropriate security management controls are applied.

9. Before use each day all equipment should be checked for any obvious signs of tampering. Any suspicious matters should be reported to the local security staffs without delay and the equipment is not to be used until checked and cleared. The fitting of frangible security seals to the body of the machine in suitable positions to prevent surreptitious access will simplify the daily checks. In the event of any emergency evacuation of the area, the DISKFAX is, if possible, to be left in a secure condition.

Transmission Security

10. **Insecure DISKFAX.** The protective marking of material which may be transmitted via DISKFAX is in accordance with the current MOD rules for transmission over "dial-up" lines without cryptographic protection, ie:

Within Mainland UK - RESTRICTED (does not include NATO RESTRICTED)

To/From Northern Ireland - UNCLASSIFIED

Rest of World - UNCLASSIFIED

Note that material marked (PERSONAL) is to be treated as RESTRICTED. Data marked "Personal for" or "Controlled Distribution only" is not to be transmitted via DISKFAX without special security authority as this needs to be protected to the same level as SECRET material.

11. **Secure DISKFAX.** A secure DISKFAX is defined as a DISKFAX connected to a specific Government approved enhanced grade cryptographic device in a configuration approved by the Communications Electronic Security Group (CESG).

12. When a secure DISKFAX is required the appropriate communications and security authorities must be consulted and their approval obtained before the equipment is procured and installed. Normally, secure DISKFAX systems are approved to carry information protectively marked CONFIDENTIAL and below. Where a user has a requirement to pass a higher protective marking or caveated information, specific endorsement must be sought from the Defence ComSec Operating Authority at DCSA on a case by case basis.

13. Secure DISKFAX installations must conform to physical and communication security criteria. No alterations are to be made to a secure facsimile installation without the approval of the IDA and relevant Principal Security Advisor (PSyA).

14. Each DISKFAX is to bear a notice indicating the highest protective marking of material that can be passed over the system, in accordance with the following:

a. For insecure DISKFAX as per **Chapter 18 ;**
b. For secure DISKFAX the notice is to read:

`NOT TO BE USED FOR TRANSMITTING DOCUMENTS PROTECTIVELY MARKED HIGHER THAN CONFIDENTIAL. `Violations of Transmission Security are to be reported immediately to the Controlling/Supervising Officer, Branch Security Officer or Unit Security Officer'.

Signed:..... Controlling Officer:..... Date:.....

Signed:..... COMSEC Authority:..... Date:.....

Transmission Procedures

15. Before transmission, the data recorded on the diskette is to be examined using suitable utilities capable of displaying or block printing the entire contents to ensure that, because DISKFAX transmits the entire contents of the diskette, only files intended for transmission have been recorded and that the highest protective marking recorded does not exceed the limits set out in paragraphs 6 and 8 above.

16. Each document to be transmitted must be recorded on a 'DISKFAX Transmission proforma' and be correctly authorized. An example of the proforma is attached below. Proformas are to be retained in the sending office for auditing purposes.

17. **Authentication.** DISKFAX machines must use dial-up telephone lines in conjunction with a telephone handset. Voice authentication with the intended recipient is to be established prior to transmission. Once the material has been transmitted voice contact is to be made to ensure that the material has been received. These procedures will ensure that material is not transmitted to an unauthorised address.

18. The DISKFAX machine is to be disconnected once the transmission has taken place.

Receipt Procedures

19. Upon receipt of material via DISKFAX, the Controller is to ensure that the received data is downloaded only on to diskettes of the type specified in paragraph 21.

20. All received material must be virus checked before it is downloaded into the recipients system. All material is to be checked for viruses before being transmitted.

Diskettes

21. A separate set of diskettes is to be maintained specifically for use with the DISKFAX; they are to conform to existing MOD policy for the use of colour coded diskettes and are to be clearly identified on the label with the word "DISKFAX" followed by a sequential serial number. Only diskettes issued by the DISKFAX Controller and appropriately marked are to be used in the DISKFAX machine. Privately owned diskettes are NOT to be used.

22. Diskettes for use on the DISKFAX machine are to be held by the DISKFAX Controller and issued as required within the Directorate/Branch/Unit. The issue is to be controlled by the Controller and, after transmission or downloading, the diskettes are to be re-formatted and returned to the controller for safe custody.

23. To ensure that no residual data remains on a diskette, each diskette is to be cleared of data with an approved package or with a disk reformat after each transmission. **Standard file deletion procedures or utilities are not acceptable for this purpose.**

Repair, Maintenance and Disposal

24. When no longer required, DISKFAX with integral hard disks should have the hard disks removed and physically destroyed if the equipment has been used to transfer any material protectively marked RESTRICTED or above.

Protective Marking	

DISKFAX TRANSMISSION PROFORMA

From:	To:
Telephone No:	Telephone No:
Reference No:	Date:
Authorised by: Name:	Rank:
Transmitted by: Name:	Rank:

This disk has been checked to ensure that only the files listed below are present.

Details of disk contents:

File Name	**Protective Marking**

Signed: Name: Rank:

Protective Marking	

ANNEX C TO

CHAPTER 19

SPECIMEN FACSIMILE SECURITY OPERATING PROCEDURES

1. Facsimile Controllers are required to produce Security and Operating Procedures applicable to their facsimile terminal. The following is a skeleton covering those points that must be addressed in the SyOPs. It is not intended to be restrictive but contains the minimum information around which the facsimile controllers can base their particular instructions. The items enclosed in inverted commas can be used verbatim. Applicability of items is shown in brackets against relative headings.

Facsimile Security and Operating Procedures

2. **Applicability.** (All facsimile). A statement as to which facsimile and to which users the SyOPs applied, eg

> "These instructions are applicable to the facsimile terminal located in Room .....Building..... and are to be read by all persons using the machine".

3. **Facsimile Controller.** (All facsimile). The facsimile Controller is:

Name:.....Dept:.....Room:.....Tel No.....

The Deputy Controller is:

Name:.....Dept:.....Room:.....Tel No.....

4. **Facsimile System.** (All facsimile). This should be description of the system and whether it is secure of insecure.

"The secure facsimile terminal consists of a "list of authorized users is shown at Annex A. Any person not shown on this list, wishing to use the facsimile machine may only do so with the approval of the Facsimile Controller".

5. **Authorised Users.** (All facsimile). "A list of authorized users is shown at Annex A. Any person not shown on this list, wishing to use the facsimile machine may only do so with the approval of the Facsimile Controller."

6. **Directory of Users.** (Secure facsimile). "A directory of secure facsimile users which can be contacted from this terminal shall be held by the Facsimile Controller".

7. **Protective Marking of Material that can be Transmitted or Received.** (All facsimile). Under this heading this should be a clear statement of the highest protective marking of material that can be sent/received over the facsimile machine. This is in addition to any notices that are displayed on the facsimile terminal.

8. **Administrative Procedures.**

a. **Secure**. "Each document for transmission over facsimile is to be accompanied by a MOD Form F Sigs 927 on which the transmission has been authorized by a person of the appropriate rank/grade. The F Sigs 927 and document must be brought to the Facsimile Controller's attention for approval before transmission" (unless the terminal is to be operated by a person listed at ANNEX A).

b. **Insecure**. "Each document for transmission over facsimile is to be accompanied by a MOD Form F Sigs 927, or a FAX "Post It" note, or have been stamped. Authorization for the transmission by a person of the appropriate rank/grade is to be included. The authorization and document must be brought to the Facsimile Controller's attention for approval before transmission" (unless the terminal is to be operated by a person listed at ANNEX A).

9. **Physical Security.** (All facsimile). This section should contain instructions for the security of the equipment when left unattended, details of where keys are held and procedures to be carried out at cease work.

10. **Transmission Procedures.** (All facsimile). A brief statement as to how to operate the machine. This is normally supplied by the system sponsor or equipment supplier in the form of a handbook.

a. "Before transmitting protectively marked information or material that bears a caveat, you should confirm with the Facsimile Controller that the facsimile terminal is approved for such purposes".

b. "After dialling the required number, make sure you have been connected to the correct destination".

c. **Secure.** "Where the material to be transmitted is TOP SECRET or bears a Special Handling Caveat, notify the Facsimile Controller who will advise on the arrangements for Authentication Procedures to be carried out".

d. "After transmission has been successfully accomplished, ensure that all protectively marked material, including waste is removed from the terminal and correctly disposed of. Unclassified waste only should be placed in waste bins".

11. **Transmission difficulties or Faulty Equipment.** (All facsimile). "If difficulties are experienced whilst using the facsimile equipment, notify the Facsimile Controller".

12. **Security Violations.** (All facsimile).

a. "If you receive a document, or part of a document, with a protective marking or Special Handling caveat for which the facsimile terminal is not approved, you must notify the Facsimile Controller immediately who will take the necessary reporting action. The facsimile controller will require copies of the material".

b. "If you transmit a document or part of a document for which this terminal is not approved, you must report the fact to the Facsimile Controller immediately". The Controller will then take the necessary reporting action.

c. "Do not attempt to hide any violation of transmission security. If the fact is known, action can be taken to minimize any damage caused".

Date:.....

Signature of Facsimile Controller.....

This page intentionally left blank.

ANNEX D TO

CHAPTER 19

SPECIMEN DISKFAX SECURITY OPERATING PROCEDURES

1. DISKFAX Controllers are required to produce Security and Operating Procedures applicable to their DISKFAX terminal. The following is a skeleton covering those points that must be addressed in the SyOPs. It is not intended to be restrictive but contains the minimum information around which the DISKFAX Controllers can base their particular instructions. The items enclosed in inverted commas can be used verbatim. Applicability of items is shown in brackets against relative headings.

Diskfax Security and Operating Procedures

2. **Applicability**. (All DISKFAX). A statement as to which DISKFAX and to which users the SyOPs applies, eg

> "These instructions are applicable to the DISKFAX terminal located in Room .....Building..... and are to be read and complied with by all persons using the machine".

3. **DISKFAX Controller**. (All DISKFAX). The DISKFAX Controller is:

Name:.....Dept:.....Room:.....Tel No.....

The Deputy Controller is:

Name:.....Dept:.....Room:.....Tel No.....

4. **DISKFAX System**. (All DISKFAX). This should be description of the system and whether it is insecure or secure eg

> This DISKFAX terminal is an insecure/secure system consisting of a DISKFAX .....serial number....., connected to extension..... on the .....exchange.

5. **Authorised Users**. (All DISKFAX). "A list of authorized users is shown at Annex A (of the SyOPs). Any person not shown on this list, wishing to use the DISKFAX

machine may only do so with the approval of the DISKFAX Controller."

6. **Directory of Subscribers**. (All DISKFAX).

a. **Insecure**. "A directory of MOD and Military DISKFAX subscribers shall be available at the DISKFAX terminal point".

b. **Secure**. "A directory of secure DISKFAX subscribers who can be contacted from this terminal shall be held by the DISKFAX Controller".

7. **Protective Marking of Material that can be Transmitted or Received**. (All DISKFAX). Under this heading there should be a clear statement of the highest protective marking of material that can be sent/received over the DISKFAX machine. This is in addition to any notices that are displayed on the DISKFAX itself.

8. **Administrative Procedures**. (All DISKFAX). Two (2) DISKFAX Registers are maintained at this DISKFAX terminal point; one for incoming and one for transmitted information. Each user is responsible for noting the details of any DISKFAX sent, or received and unloaded by them, in the appropriate register. (Specimen layouts for the Transmission and Receipt/Unload Registers are attached: these may be reproduced and used in a loose-leaf binder, or the format may be transferred to a suitable ruled A4 book if preferred.)

9. "Each disk for transmission over DISKFAX is to be accompanied by a proforma on which the transmission has been authorized by a person of the appropriate rank/grade. The proforma and diskette must be brought to the Facsimile Controller's attention for approval before transmission" (unless the terminal is to be operated by a person listed at ANNEX A).

10. **Physical Security**. (All DISKFAX). This section should contain instructions for the security of the equipment when left unattended, the checks to be made for tampering, details of where keys are held and procedures to be carried out at cease work.

11. Normally after the completion of a transmission or downloading after a reception the machine is to be disconnected. In special cases, the security and communications authorities may authorize unattended out of hours working in the `receive mode only' provided that:

a. The equipment is in a designated secure area or locked room.

b. Appropriate security management controls are applied.

12. **Diskettes.** (All DISKFAX). "A separate set of diskettes is to be maintained specifically for use with the DISKFAX; they are to conform to existing MOD policy for the use of colour coded diskettes and are to be clearly identified on the label with

the word "DISKFAX" followed by a sequential serial number. Only diskettes issued by the DISKFAX Controller and appropriately marked are to be used in the DISKFAX machine. **No other diskettes are to be used**."

13. "Diskettes for use on the DISKFAX machine are to be held by the DISKFAX Controller and issued as required within the Directorate/Branch/Unit. The issue is to be controlled by the Controller and, after transmission or downloading, the diskettes are to be re-formatted, to ensure that no residual data remains on a diskette, and returned to the Controller for safe custody. **Standard file deletion procedures or utilities are not acceptable for this purpose.**"

14. **Transmission Procedures**. (All DISKFAX). A brief statement as to how to operate the machine. This is normally supplied by the system sponsor or equipment supplier in the form of a handbook.

15. Only diskettes from the separately maintained pool for use on the DISKFAX are to be used.

16. Copy or save the file(s) to be transmitted onto an empty disk. Only files for one recipient should be batched together; where there are files for more than one recipient either:

a. Prepare a separate disk for each recipient; or

b. Make multiple transmissions, altering the details in the identification file between transmissions.

17. Create a standard identification file called, for example, "OODETAIL" using a word processing package, and which must contain the following information:

a. A title;

b. The identity of the originator;

c. The identity of the intended recipient;

d. The number of files on the disk (including "OODETAIL");

e. For each file, its name and a brief description.

18. This file in the above format must be created even when only one data file is being transmitted. The total number of bytes occupied by the files should also be noted.

19. DISKFAX machines must use dial-up telephone lines in conjunction with a

telephone handset. Voice authentication with the intended recipient is to be established prior to transmission. Once the material has been transmitted voice contact is to be made to ensure that the material has been received. Details of the transmitted DISKFAX to be given are, the date and time of the transmission, the volume and protective marking of data transmitted. The last item is to ensure that the correct coloured coded receiving diskette is used.

20. The transmission whether successful or not must be recorded in the register.

21. **Receiving/Unloading Information**. (All DISKFAX)

a. **DISKFAX with diskette drive only**. When notified by a sender that information is to be "faxed", the DISKFAX Controller will issue a blank, formatted diskette. The diskette must be inserted into the DISKFAX terminal prior to the data being sent. When the data has been received, note the details of the machine from which it was transmitted, the date and time of the transmission, the volume and protective marking of data transmitted.

b. **DISKFAX with in built hard disc**. This type of DISKFAX automatically stores incoming transmissions on an in-built hard disk. The UNLOAD function allows a user either to remove a transmission from the hard disk to a diskette, or simply to check what messages are available. Once unloaded the stored message is no longer available on the DISKFAX. A blank, formatted diskette is to be issued by the Controller for unloading. Ensure that the disk capacity is adequate for the volume of data transmitted. The same details of the reception as at a. above are to be noted.

22. The details of receptions/unloads are to be entered into the register held at the terminal point.

23. **For DISKFAX with Fixed hard Disc**. Once a message has been unloaded to a diskette, it cannot be unloaded a second time. It is essential that immediately a transmission has been unloaded, the identification file is checked to ensure that the correct one has been unloaded. If the correct transmission has been unloaded, the sender should be notified of receipt of the transmission. If, however, a transmission intended for another recipient has been unloaded, the floppy disk must be passed to the correct recipient immediately. A different blank disk must then be used to unload the correct transmission.

24. If an expected transmission cannot be found on the hard disk list, inspect the unload register to see if a transmission matching the one expected has been unloaded. If it has, contact the person who unloaded it. If any transmission is "misplaced", immediately report the facts to the DISKFAX Controller or Deputy Controller.

25. All received material must be virus checked before it is downloaded into the recipients system.

26. **Transmission difficulties or Faulty Equipment**. (All DISKFAX). "If difficulties are experienced whilst using the DISKFAX equipment, notify the DISKFAX Controller".

27. **Security Violations**. (All DISKFAX).

a. "If you receive a document, or part of a document, with a protective marking or Special Handling caveat for which the DISKFAX terminal is not approved, you must notify the DISKFAX Controller immediately who will take the necessary reporting action. The DISKFAX Controller will require copies of the material".

b. "If you transmit a document or part of a document for which this terminal is not approved, you must report the fact to the DISKFAX Controller immediately". The Controller will then take the necessary reporting action.

c. "Do not attempt to hide any violation of transmission security. If the fact is known, action can be taken to minimize any damage caused".

Date:..... .....
Signature of DISKFAX Controller

LIST OF APPROVED DISKFAX SYSTEMS

System No	Phone No	Internal Name	Location	Controller Name	Controller Phone	Deputy Controller Name	Deputy Controller Phone

NOTE 1 - The system number is also the "Short-Code" dialling code for the system, ie when the DISKFAX shows "RECALL:"

the code to be entered is the system number shown above.

DISKFAX TRANSMISSION REGISTER

System Name: **System Number:**

Time	System no sent to	Volume sent(k)	Sent ok ?	Intended Recipient	Sender		
					Name	Branch	Signature

DISKFAX RECEIPT/UNLOADING REGISTER

System Name: **System Number:**

Time Unloaded	Message details					Unloaded by		
	Seq No	Sent from	Date	Time	Volume (k)	Name	Branch	Signature

VIDEO SECURITY

Part 4: Violations and Compromises

CHAPTER 20

VIDEO SECURITY

Part 1: The Transmission of Still Photographic Images Containing Protectively Marked Information

Introduction

2001. **SPI systems**. SPI systems allow visual (still image) or audio transmission between sites, but not simultaneously. SPI systems currently have no network capability. Use of a modem allows digital information conversion and compression, thus enabling its use over analogue, cellular or RF links, using bandwidths as low as l6kbit/s (this does not however prevent its use over ISDN or kilostream/megastream lines). Storage and printing of these images is achieved via normal PC functions. SPI systems are telephones that have a camera and screen to permit the transmission of photographic images when the telephone is not being used for voice. The system also incorporates the use of standalone PC technology to store and manage photograph files. The camera can be used to transmit images of either hand-held documents, equipments, persons or items on a background.

2002. SPI systems are subject to the same COMSEC, TEMPEST and procedural security considerations as other telephone equipment and should only be used within the limit of the protective marking for which the equipment and the transmission are authorised. The limit of protective marking for the transmission is determined by the location of the transmitting and receiving equipment, the transmission medium and the accreditation of the. local exchange. Additionally, because PC based storage and management software is used within the SPI system, each equipment of this kind requires Security Policy Documentation, as laid down at **Chapter 3**, which will normally be a System Security Policy (SSP) and Security Operating Procedures (SyOPs), similar to those necessary for Secure Fax and DiskFax systems.

Protective Marking Labels

2003. If SPI systems are being used to transmit protectively marked images, care is to be taken to ensure that the protective marking is visible in the image transmitted and that the recipient is aware of the protective marking.

Unintentional Background Display

2004. Anyone using an SPI system should be aware of the risk that the camera could transmit information displayed behind the subject and therefore care should be taken

when considering the position of the subject and camera direction. This is especially the case in open plan offices. A visual warning that SPI equipment is in use may need to be displayed on the door to an office or close to where the transmission is occurring in an open plan area.

Sector Control

2005. While experience is being gained with this relatively new technology, all requirements for the procurement of SPI systems should be approved by the relevant Principal Security Advisor in consultation with CIDA.

Part 2: CCTV

Introduction

2006. This section covers CCTV where information is processed by cable and not by video base-band transmission or radio frequency carrier.

Description

2007. CCTV provides a reasonable degree of security provided that the master and the monitors and all their lines are wholly contained in a secure building. The technical security risks comprise:

a. The interception of information following a deliberate attack on line or system.

b. TEMPEST.

2008. In many cases one master unit serves a number of monitors in different locations. When showing protectively marked information the security of all the monitors is to be taken into account. If the monitors are left permanently in one position the power supply is to be fitted with an approved security cover secured by approved padlock. The transmission cable is to be permanently sealed to the TV aerial jack. The CIDA must approve all such installations.

2009. If monitors are stored elsewhere and are only connected for specific programmes the security of all transmission cable aerial connectors is to be taken into account. They are all to be fitted with an approved security cover secured by an approved padlock. (It is possible to record a programme direct onto a video cassette recorder without using a TV.)

2010. **Video Tapes**. These should be stored in a manner appropriate to their protective marking. (See JSP 440 Vol I Chapter 5 Section 1 Annex A).

Part 3: Secure Video Conferencing

Introduction

2011. **Video conferencing systems**. Video conferencing allows visual (moving image) and audio transmission simultaneously between sites, permitting near normal person to person communications or small meetings to be held between distributed groups. To allow this duplex operation, it invariably requires one ISDN2 line offering a minimum bandwidth of l28kbit/s (two channels at 64kbit/s).

2012. Video conferencing allows visual and audio transmission between sites, permitting near normal person-to-person communications or small meetings to be held between distributed groups.

2013. Advances in technology, in particular compression techniques, have reduced the transmission bandwidth requirement substantially, bringing it within the capacity of cheaper cryptographic equipment. The International Telecommunications Union (ITU) Telecommunications Standardization Sector (TSS) has set a common international video conferencing standard.

2014. All secure video conferencing and cryptographic equipment combinations must meet the National and Departmental TEMPEST guidelines contained in **Chapter 21**.

2015. Where NATO classified information is also to be handled, the equipment must also meet the NATO guidelines contained in MC315.

2016. Where a conflict arises between the assessed national and NATO local threat levels, the TEMPEST standards appropriate to the higher threat level are applicable.

2017. All items of video conferencing equipment must be compatible with the standards encompassed within ITU/TSS H.32O. NATO has adopted ITU standards to facilitate interoperability between nations. There are separate audio transmission standards mandated for narrowband and wideband systems (bandwidth 2 Mbits/s and above) in ITU/TSS H.320 recommendations . An operational audio transmission standard G.728 is also available and is suitable for use with both systems. To provide interoperability between video conferencing systems, it is recommended that the operational audio standard G.728 is provided on MOD procured items of video conferencing equipment.

2018. Secure video conferencing terminals may, if required, use approved recording equipment.

Installation Policy

2019. Secure video conferencing systems must be installed in accordance with the TEMPEST regulations.

a. The installation must be certified by the relevant Co-ordinating Installation Design Authority (CIDA).

b. The installation must be in accordance with either AMG719 or JSP480, as appropriate.

2020. Video conferencing locations can be connected either by Public Telephone Terminal (PTT) or Service provided digital bearers. Video conferencing connectivity may be achieved in one of the following configurations:

a. Point-to-Point.

b. Multi-Point.

Point-to-Point

2021. Point-to-point transmissions made between stand alone video conferencing systems must be protected by a means designed to ensure their security. Video conferencing systems require the same level of protection of transmission paths as other communications media, in accordance with current regulations.

Multi-Point

2022. Multi-point Secure Video Conferencing (MPSVC) systems may be required in various military and government organisations and military locations world-wide. It is envisaged that MPSVC facilities will be utilised as a common user facility available to all staff, with the appropriate security clearances, in the pursuance of their duties. Connectivity of MPSVC systems will be achieved through a multi-point control unit (MCU) sited at a suitable location in the communications network. The MCU may be accessed by either dial-up or permanent private wire (PW) connection. Consideration should be given that as a common user facility, the protective marking of a conference may vary from UNCLASSIFIED through to TOP SECRET codeword. In this case transmissions between users must be protected to the highest potential protective marking to be used, and it may therefore prove more financially expedient to purchase High Grade (HG) system at the outset rather than identify funds to update later.

2023. System sponsors should alert cryptographic sponsors to their needs as early as possible because of the long lead times associated with the provisioning of cryptographic products.

2024. Funds are not to be committed to equipment procurement until an SSP has been produced and agreed to the satisfaction of the accreditor as a satisfactory basis upon which to proceed.

Documentation Requirement

2025. All MPSVC systems handling protectively marked information are to have an Security Policy Documentation (SPD) in accordance with **Chapter 3**. The SPD is to be produced by the system project office or sponsor, to the satisfaction of the accreditor(s), and will be used as the basis of accreditation of the system by the appropriate the Principal Security Advisor or the DSSO. Point-to-point systems utilizing bulk encryption techniques or a secure telephone for security protection need only produce Terminal Security Operating Instructions. Point-to-point users who join an existing MPSVC system on an occasional basis must ensure full compliance with the MPSVC system SPD prior to use.

2026. The SPD set produced must include Security Operating Instructions applicable to individual terminal installations and approved by the relevant unit/branch security officer.

System Sponsors Responsibilities

2027. The system sponsor has the following security responsibilities:

a. The appointment of a System Design Authority, if the planned system is complex ;

b. Obtaining Co-ordinating Installation Design Authority approval ;

c. Provision of terminal and cryptographic equipment ;

d. Co-ordinating key material requirements with the Defence COMSEC Authority at DCSA ;

e. System operating policy .

f. Liasing with Branch/Unit Security Officers to appoint terminal controllers.

g. Producing the SPD ;

h. Obtaining accreditation.

2028. System Sponsors are:

a. Tri-Service operational systems – EC(CCII)

b. RN systems - DCIS(N)

c. Army systems - Budget Holders. DCIS(A) will advise Sponsors on TEMPEST and cryptographic issues.

d. RAF systems - DCIS(RAF)

e. MOD HQ systems - DCSA DII

Terminal Security Officer (TSO)

2029. The TSO is a suitably cleared person responsible to his establishment security officer for day-to-day control of a secure video conferencing terminal. In particular he is responsible for security of the terminal and its usage, including the issue of Security Operating Instructions which are mandatory for all secure video conferencing terminals.

Unintentional Background Display

2030. Anyone using a video conferencing system should be aware of the risk that the camera could transmit information displayed behind the subject and therefore care should be taken when considering the position of the subject and camera direction. This is especially the case in open plan offices. A visual warning that video conferencing equipment is in use may need to be displayed on the door to an office or close to where the transmission is occurring in an open plan area.

Part 4: Violations and Compromises

Compliance

2031. Compliance checks, including routine COMSEC monitoring for transmission violations, may be carried out against all MOD video systems in accordance with **Chapter 12**.

Incident Handling

2032. Any security incidents affecting video systems must be handled in accordance with the regulations relevant to the installation, and a report raised to the Joint Security Co-ordination Centre (JSyCC), through the appropriate Monitoring and Reporting Centre (MRC) where applicable, in accordance with **Chapter 11**.

RADIATION SECURITY (RADSEC)

CHAPTER 21

RADIATION SECURITY (RADSEC)

Introduction

21001. Radio frequency (RF) waves are forms of Electromagnetic Radiation (EMR), and their presence in the environment, both as a matter of design in sensor (e.g. radar) and communications systems, and as a consequence of the fundamental electronic design of CIS equipments, present potential security issues in terms of Confidentiality, Integrity and Availability.

21002. The discipline of Radiation Security (RadSec) is therefore aimed at managing the risks associated with RF signals, both intentional and unintentional, under the following 3 major sub-disciplines :

a. TEMPEST ;

b. ELSEC ;

c. RFSEC.

21003. The security of data deliberately modulated upon RF signals is covered within the Communications Security (COMSEC) discipline, typically by the use of cryptographic systems, as laid down at **Chapter 23**. A diagram providing a high level illustration of the inter-relationships with other Information Security disciplines in the context of RadSec is given at **Annex A**, with fuller details of the non-technical aspects of Information Security are given at **Chapter 1**.

Responsibilities

21004. UK national RadSec policy is the responsibility of the Cabinet Information Systems Security Policy Committee (SO(IS)): the authority for advising on the implementation of this policy, including the provision of TEMPEST and ELSEC standards for the testing of equipment and installations, lies with CESG. CESG liases closely with the Security Service and other appropriate authorities, which are responsible for assessing the overall threat and for advising on the need for countermeasures.

21005. Responsibility for assessing the threat, vulnerability, and hence the risk, and deciding on the countermeasures for projects/systems, lies with the Departmental Security Officer (DSO) through the security chain of command.

SECTION 1 - TEMPEST

21006. **Emissions** All electrically-powered equipment is liable to produce unintended electromagnetic signals. Compromising emanations are unintentional data-related or intelligence-bearing signals which, if intercepted and analysed, disclose protectively marked information being transmitted, received, handled, or otherwise processed by information processing equipment, system or platform.

21007. The investigation and study of compromising emanations is called "TEMPEST". The term "TEMPEST" is also used to encompass these phenomena themselves and the measures for their suppression. *(Note: The term "TEMPEST" is **not** an acronym).*

21008. Equipment used for information processing may emit signals that are compromising. Such compromising emanations may be propagated through space, along nearby conductors, and by other unintended transmission channels. The interceptability, propagation ranges and analysis of these emanations are affected by a variety of factors, e.g. the functional design of the information processing equipment, its installation, physical and associated personnel security, as well as the electromagnetic ambient noise conditions.

21009. Therefore, a number of technical measures can and should be applied to suppress compromising emanations which would otherwise be vulnerable to interception and hence to exploitation.

EMC

21010. Electromagnetic Compatibility (EMC), which describes the undesirable effects of mutual interference between devices, addresses many of the same concerns as TEMPEST, albeit generally to less rigorous standards. The main EMC emission effects are:

a. Mains supply current distortion and/or transients, or Radio Frequency Interference (RFI), generated within the equipment and conducted out via the mains supply;

b. Current transients or RFI, generated within the equipment and conducted out via the signal leads or other equipments;

c. EMR generated and emitted directly from the equipment circuitry, enclosure(s) and cables(s).

21011. **Susceptibility and Immunity** Electrically-powered equipment is **susceptible** to being affected by other sources of electromagnetic radiation (EMR), leading to

distortion of data (potential breach of information Integrity) or disruption of service (potential denial of service).

21012. A system's ability to withstand such effects is referred to as **immunity**, and the effects addressed are:

a. Supply voltage drop-outs, dips, surges and distortion ;

b. Transients and RFI conducted into the equipment via the mains supply ;

c. Radiated transients or RFI, conducted into the equipment via signal leads;

d. RFI picked up directly by the equipment circuitry ;

e. Electrostatic discharge.

21013. Collectively, these issues are referred to as Electromagnetic Vulnerability (EMV).

Responsibilities

21014. Overall responsibility for assessing the TEMPEST threat, vulnerability, and risk, lies with the MOD TEMPEST Authority, InfoSy(Tech), on the staff of the Departmental Security Officer (DSO), and is implemented through the security chain of command.

21015. Responsibility for the selection of countermeasures for individual systems lies with Project Managers and or System Operating Authorities (SOA), but the individual threat assessment process is a matter purely for the security authority.

21016. For shared UK/NATO facilities, the TEMPEST authority shall be decided on a case by case basis by the host nation. For UK national assets that process NATO information, the authority is CESG or its delegated representative.

21017. In order to allow flexibility and assure the cost-effective application of TEMPEST countermeasures, a series of documents has been developed within NATO by the Communications and Information Systems Security and Evaluation Agency (SECAN) on behalf of the Military Committee.

21018. These documents provide test standards for laboratory evaluations of equipment and systems, test procedures for the evaluation of tactical mobile platforms, facility attenuation characterisation, and installation guidelines. These documents represent a technical basis for the UK TEMPEST programme. By selectively using these documents, in an integrated cohesive manner, the most cost-effective level of TEMPEST security can be achieved.

21019. In addition to the security and project management staffs, a number of roles are identified within MOD as having specific TEMPEST responsibilities.

21020. **Co-ordinating Installation Design Authority (CIDA)**, or their delegated representatives, are responsible for endorsing the design of an installation to store, process, or forward process official information for a building or establishment.

21021. **Platform TEMPEST Control Authority (PTCA)**, or their delegated representatives, are responsible for endorsing the design of an installation to store, process, or forward process official information for mobile platforms (e.g. ship, vehicle or aircraft).

21022. Details of the MOD CIDAs and PTCAs are given at **Annex B**.

21023. Subordinate to the CIDAs are a number of different types of technical staffs, all of whom have some involvement in ensuring that Installations are properly performed or maintained:

a. Site CIDA (SCIDA);

b. Technical Supervisory CIDA (TSCIDA);

c. System Design Authority (SDA);

d. Delegated SDA (DSDA);

e. System Designer (SD);

f. Installation Design Authority (IDA);

g. Delegated IDA (DIDA);

h. Installation Designer (ID);

21024. Not used.

21025. The identification and measurement of electronic emissions is the task of specialist teams, which may be provided by the MOD or external agencies, such as CESG. Security staffs are to be consulted on the frequency of TEMPEST On-Site Testing and are to make the necessary arrangements for inspection teams to visit locations/Units.

21026. **Project TEMPEST Control Officers (PTCO)**. Project Officers should be aware of the possibility of TEMPEST affecting any project for which they are responsible. If necessary, Project Officers and Establishments should consider

appointing a project TEMPEST Control Officer (PTCO); one of whose main responsibilities will be configuration control. Guidance on this topic, documentation and training is available through Principal Security Advisors (PSyA).

21027. **TEMPEST Control Officers (TCO)** For deployments away from CIDA planned or established sites, the UK commander of the deployment is responsible for configuration control of CIS containing UK national information. This configuration control is to be effected by TEMPEST Control Officers (TCO) acting with the authority of the commander. More information on TCOs is given at **Annex D**.

21028. Not used.

Risk Assessment

21029. A risk assessment is to be carried out early in the planning stages of a project in order to minimise any subsequent impact on design and cost caused by TEMPEST considerations. A similar exercise will need to be conducted when modifications to existing equipment are proposed.

21030. The risk assessment compromises a review of the generic and local threats and vulnerabilities, as is common throughout security.

21031. **Threat** Several adversaries have demonstrated a sophisticated capability to exploit TEMPEST vulnerabilities, and a willingness to conduct operations against facilities in their own countries or in countries where they can operate with some degree of freedom.

21032. However, TEMPEST attacks are expensive in resources, difficult to mount, and unpredictable in outcome. They normally require close access to the system being targeted and are therefore likely to be attempted only where all the following circumstances are met:

a. Other methods of intelligence gathering are impractical ;

b. Physical security measures are ineffective and permit an attacker to penetrate a secure perimeter ;

c. An attack is practical (i.e. the attacker can acquire a safe listening post close enough to the radiating equipment and from which he can operate undetected over an extended period).

21033. The TEMPEST Threat Assessment (TTA) to MOD facilities and equipment is provided by the Joint Security Co-ordination Centre (JSyCC) within DDefSy as part of the Information Security Threat Summary (ISTS) issued to PSyA and Co-ordinating Installation Design Authorities (CIDA). This is based upon the Annual Threat Assessment (ATA), prepared by the Security Service and published with the endorsement of the Official Committee on Security.

21034. The status of Threats, unless specifically catered for in a current ISTS, should be verified with the JSyCC Intelligence Cell (JSyCC Int) to ensure that the ISTS threat level for a particular environment is still valid.

21035. **Vulnerabilities** The likelihood, or risk, of a successful attack will depend on the extent of the perceived threat to an installation, together with the TEMPEST vulnerabilities of the equipment or system involved (i.e. its propensity to radiate). A TEMPEST attack in the UK is only likely to succeed where equipment which emits strong, easily intercepted, TEMPEST signals (notably, most models of VDU, microcomputer, wordprocessor, facsimile, electronic typewriter, video equipment and some types of printer) is used regularly to process highly protectively marked information and where nearby buildings might house a safe listening post.

21036. **Note, however, that where radio transmitters are involved, a TEMPEST related attack can be mounted far more easily and the need for close proximity no longer exists.**

21037. In all cases where radio transmitters are known or planned to be located in close proximity to MOD CIS used to store, process or forward Protectively Marked material, both the appropriate PSyA and the CIDA must be consulted in advance of any procurement action for such devices, as specific TEMPEST equipments may be required. As with all RF effects, it is important that the question of proximity of radio transmitters is considered in a Spherical manner i.e. taking account if all 3 dimensions.

21038. **Site TEMPEST Assessment** Within the MOD TEMPEST countermeasures are based on a site specific TEMPEST Countermeasure Assessment (TCA). This takes into account the threat, the vulnerability of the installation and likelihood of interception.

21039. The outcome of the TCA will dictate whether any specific measures need to be considered before equipment is purchased. Conditions vary widely between installations and as countermeasures are usually expensive (especially when applied retrospectively). The TCA may identify the need for a TEMPEST Visual Inspection (TVI) to be carried out prior to the commissioning of the installation. This will be carried out by the Sector TEMPEST Authority.

21040. Within the UK mainland, other than in certain parts of Greater London, the prevailing for TTA many years has remained at **Level 6** (Negligible), and this can be assumed to be the case unless units have been specifically advised otherwise by their PSyA. For all other locations, a bespoke TCA is to be carried out for each installation under arrangements made by the PSyA, preferably at the planning stage, <u>but in any case must be completed before any equipment is procured</u>.

21041. **Inspectable Space** Inspectable space is the three dimensional space surrounding equipment that processes protectively marked information, within which TEMPEST exploitation is not considered practical or where legal authority exists to

identify and remove a potential TEMPEST exploitation threat. Equipment TEMPEST standards may be reduced by increasing the inspectable space around the facility.

21042. **Screened Enclosures / Bunkers / EMP Hardened Facilities** Certain UK and NATO assets are located in screened enclosures, underground, or Electromagnetic Pulse (EMP) hardened facilities that inherently provide protection against the escape of compromising emanations.

21043. For such facilities which have sufficient electromagnetic radiation attenuation, equipment TEMPEST countermeasures may be significantly reduced, as long as countermeasures in accordance with AMSG-719 are applied to power lines, signal lines, fortuitous conductors and other radiators which leave the shielded area.

21044. The appropriate Co-ordinating Installation Design Authority (CIDA) should be consulted to determine if such facilities qualify for reduced TEMPEST countermeasures. In some cases screened enclosures are a cost-effective alternative to TEMPEST equipment.

21045. The staff responsible for providing specific TCAs are normally the PSyA, but in the case of **Joint Force Deployments** both PJHQ J2 and JSyCC Int should be consulted at the earliest possible juncture for a consolidated TCA.

Tempest Zoning

21046. The term Zoning is used in different contexts within TEMPEST. Within MOD, the terms Red Zone are used to designate areas where the CIDA accept compromising emanations may be present, and Black Zone is used for areas where the CIDA believe no compromising emanations may be present.

21047. NATO additionally defines “Facility zones”, which are determined by measuring the total attenuation, comprising free space attenuation, inherent to a facility, and the attenuation provided by the physical building structure, and “Equipment zones” which are obtained by comparing laboratory TEMPEST test data to specific zone limits. In the case of any desire in MOD to use the Facility/Equipment zoning techniques instead of UK Installation Control practices, both the PSyA and the CIDA must be consulted in advance.

Defensive Measures

21048. There are a number of ways in which the risks from TEMPEST attack can be reduced. In many cases, particularly where the threat is regarded as **Level 5** (Low) or **Level 6** (Negligible), prudent siting of equipment and correct installation will provide sufficient protection.

21049. The MOD minimum standards for TEMPEST countermeasures is laid down at **Annex D**. This is derived from CESG Infosec Memorandum No. 16, as interpreted for

the MOD environment. All Risk Assessments for TEMPEST requirements within Defence are to use this standard as a Baseline, and for certain instances where Special Material (e.g. Intelligence or Operations) is to be processed, Accreditors may require additional precautions.

21050. The Risk Assessment against Annex A consist of 2 elements :

a. Requirements for Equipment countermeasures ;

b. Requirements for Installation control.

21051. These are recommended minimum equipment/system requirements. If it is more cost-effective to choose equipment having lower emanation levels, this is allowed. Equipment having lower emanation levels could reduce the installation requirements. A list of Potential Vulnerabilities (PV) for equipment types and their coupling zones (CZ) is contained within a Defence Information Assurance Notice (DIAN).

21052. Security Policy Documentation (SPD) for the CIS being considered must record the results of the assessments against both these requirements, and the way in which these are to be achieved.

21053. **TEMPEST Countermeasures For Military Deployments** Although equipment to carry out TEMPEST attacks is readily available, its effective use is extremely difficult, requiring careful planning and close access. This takes time.

21054. In recognition of this, military deployments to new locations with threat levels no higher than **Level 3**, will be allowed to use Civil EMC equipment for the **first month**.

21055. Bespoke assessments of the current threat level are to be obtained from JSyCC Int prior to all UK forces deployments.

21056. Also, during this period no TEMPEST installation countermeasures will normally be required, other than for High Grade (HG) cryptographic equipment and transmitters, which should always be installed in accordance with AMSG-719.

21057. More detail on military deployments is found at **Chapter 9**, and in the requirement for the TEMPEST Control Officer (TCO), as laid down at **Annex D**.

21058. **Information Integrity and Availability** Within Electromagnetic Security, the prevention of loss of information integrity and availability is covered by the application of Electromagnetic Compatibility (EMC), which is defined in the International Electrotechnical Vocabulary (IEC 50) as:

'the ability of a device, equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment'

21059. The term function satisfactorily is interpreted here as meaning:

a. The equipment must be reasonably protected against threats to its own integrity and availability from electromagnetic disturbances generated elsewhere ;

b. The equipment must be reasonably protected against introducing into an environment electromagnetic (EM) disturbances which might compromise a nearby equipment's integrity and availability.

21060. Within the current UK mainland Threat, the use of equipments meeting both the civil (89/336/EEC) and military (DEF STAN 59-41 or US equivalent MIL-STD-461) EMC standards, although not specifically designed to provide countermeasures to loss of information integrity and availability, should provide adequate countermeasures.

Tempest Equipment

21061. The requirements for TEMPEST Certified equipments to be used within MOD will be derived from Annex D. It should be noted that the requirement for such certification relates not only to the environment but also to be Potential Vulnerability (PV) of the equipment in question, as more vulnerable equipment types will have a large Interference Zone (IZ) which may require Certification to prevent side-effects on other equipments in the vicinity.

21062. Where specific TEMPEST equipments or facilities are required to be built for MOD purposes, the guidance laid down in CESG Infosec Memorandum No. 16 (IM16) in respect of TEMPEST Certification requirements is to be followed. This will require the production of a TEMPEST Control Plan (TCP).

21063. **Security and Maintenance** It is possible to modify electrical equipment to enhance its radiation. Where the TEMPEST approved equipment is deployed, it is to be given appropriate physical protection and periodic inspections to detect tampering. Maintenance is to be carried out by, or under the supervision of, technically qualified appropriately security cleared personnel.

21064. **Disposal** Any TEMPEST Certified Equipment to be disposed of within 5 years of delivery should be crushed or have TEMPEST protection removed. Thereafter, there is no restriction on disposal.

21065. This guidance does not relate to equipment which includes other security features in addition to TEMPEST protection such as cryptographic equipment, or

equipment containing cryptographic devices which may require more stringent methods of disposal.

Installation Control and Testing

21066. Whenever TEMPEST countermeasures are assessed as necessary, the installation regulations laid down in the current edition of NATO AMSG-719 "Installation of Electrical Equipment for the Processing of Classified Information" are to be adhered to. AMSG-719 provides the facility and system installation guidelines that should be followed to achieve an acceptable degree of security at a variety of facilities. It considers factors related to physical security, separation of conductors/equipment and the TEMPEST profile of the equipment.

21067. In all other case, JSP480 – Codes of Practice for Installation Design should be followed for all MOD installations, which encapsulates Best Current Practice for installation and as such minimises the TEMPEST vulnerabilities that could be exploited by opportunist attackers.

21068. Units should retain British TEMPEST Regulations BTR/01/200, which was previously used as the minimum standard for installation practice, to cover Legacy installations until they are replaced with installations implemented in accordance with either AMSG-719 or JSP480 as appropriate.

21069. Design of an installation to store, process, or forward process official information must be endorsed by the relevant Co-ordinating Installation Design Authority (CIDA) or their delegated representative, for the building or establishment, or the Platform TEMPEST Control Authority (PTCA) for mobile platforms (e.g. ship, vehicle or aircraft).

21070. Installation will be verified as being in accordance with current TEMPEST regulations, and an Installation Design Conformance Certificate (IDCC) will be issued. Once such an installation has been certified, no changes can be made to the configuration of the system or layout of the area in which it is installed without approval from the CIDA.

Platform Tempest Qualification

21071. For tactical mobile scenarios, involving the processing of protectively marked information at CONFIDENTIAL level and above, equipment and systems meeting AMSG-784 Volume 1 will normally be required and platforms should be tested in accordance with AMSG-784 Volume 2.

21072. In such cases, the guidance laid down in CESG Infosec Memorandum No. 16 in respect of TEMPEST Qualification requirements is to be followed, which will require

the production of a TEMPEST Control Plan (TCP) by the Project Office, working in conjunction with the PRCA.

Tempest Control Plan (TCP)

21073. The TCO is to ensure that no unauthorized changes are made to any system which will affect the requirement for TEMPEST countermeasure. The basis of the TEMPEST control strategy is the TEMPEST Control Plan (TCP), which the TCO is to devise, implement and maintain. The minimum contents required of a TCP are at **Annex E**.

Compliance Checking

21074. Where a TCA has given leeway to procure non-TEMPEST certified equipment subject to a post installation TEMPEST On-Site Test (TOST), the necessary testing is arranged through the CIDA in conjunction with the PSyA. Some projects may also identify the need for a TOST where TEMPEST equipments have been used.

21075. Post-test reports are forwarded to the PSyAs who will specify whether any remedial action is necessary. Further details on such activities are given at **Chapter 12**.

Incident Handling

21076. Compromises of TEMPEST should be reported, as with all other Information Security concerns, in line with the requirements of **Chapter 11**.

Further Advice

21077. The MOD source publication, in addition to this Manual, which details the basic Installation Design requirements is :

JSP480 - "CIDA Codes of Practice"

21078. The national / NATO source publications, such as CESG Infosec Memorandum No. 16 (IM16), which detail the TEMPEST requirements are issued by CESG to recipients as approved by InfoSy(Tech). Most MOD units will not require access to these, but should this be required, the InfoSy(Tech) must be approached to endorse the distribution request.

SECTION 2 - ELSEC

Electronic Emission Security (ELSEC)

21079. The measures taken to prevent interception and exploitation of those intentional electromagnetic emissions not produced specifically for communications purposes are broken down into Electronic Emission Security (ELSEC) and Radio Frequency Security (RFSEC). Although related disciplines, ELSEC is the subject of this section, and RFSEC is covered in Section 3.

21080. The purpose of ELSEC is to protect the limited set of RF emission characteristics that attract a protective marking of CONFIDENTIAL and above, including those which have designated Wartime Reserve Modes (WARM) which can be protectively marked up to SECRET. The premature emission of this information may enable a hostile group or country to develop both a similar capability and more effective Electronic Countermeasures (ECM), more quickly and effectively than desired.

Overview

21081. The interception of Radio Frequency (RF) transmissions of every type is an attractive and profitable source of intelligence, in particular because the large theoretical propagation distances as detailed at **Chapter 26** means it can in principle be undertaken from the safety of home territory; international air space; or the high seas; and from foreign diplomatic and trade premises, or during other activities, in the United Kingdom.

21082. In the context of non-communications electromagnetic emissions, RF interception could reveal information relating certain aspects of the electronic techniques employed in the equipment; the extent and preparedness of the country's defences, and the capacity of its industrial resources which is otherwise protected by physical, personal and CIS security measures.

21083. The nature of the Threat environment means that the requirements for ELSEC measures currently necessary are only those required to counter the ELINT (Electronic Intelligence) element of any SIGINT (Signals Intelligence) gathering activities by a hostile group or country.

21084. The aim of ELSEC practices is to minimise, as far as possible, the risk of compromise of emission information that would in itself be protectively marked CONFIDENTIAL and above, by limiting the opportunities for its interception by any hostile group or country. Total denial is impracticable in most cases without seriously impeding the progress of a project through its developmental stages and more so when operational. Emitters must emit; but the security aim must be to assess the risk and implications of compromise by interception and then to apply protective measures

commensurate with protective marking, the characteristics of the emission, and the local conditions.

21085. The protective marking associated with information obtainable from interception of non-communications electronic emissions, is generally considered to be higher in the early stages of research and development. Although it may not be practicable to maintain the same degree of security from the beginning of development of equipment to the in-service date and beyond, continuation of security is essential.

21086. The technical analysis of such emissions can provide data which may also allow development of similar equipment or systems, but also effective electronic countermands (ECM). These may involve sophisticated deception and decoy techniques or jamming. Indeed successful interception and analysis could allow the development and deployment of countermeasures to coincide with the operational use of the target signals.

21087. The intercept of only seconds of a complex signal can provide vital information as to its purpose, modes and technical characteristics. Generally speaking, a high signal level is necessary for analysis but even low level will alert an interceptor to a signal of interest and for subsequent attempt at intercept he can then maximise his resources. Weaknesses or exploitable features, which may not be evident to the developer, may give hostile analysts an early lead in designing countermeasures.

21088. The system types for which RF emissions will need to be considered for ELSEC are radars, including those used for:

a. Surveillance ;

b. Target acquisition ;

c. Missile Guidance and Control ;

d. Shell Tracking ;

e. Fuzing Systems.

21089. The interception of occasional individual emissions is of relatively small importance; the main object should always be to avoid the development of patterns of events which, either of themselves, or in conjunction with easily obtained collateral, reveal sensitive information such as:

a. The purpose of the signal ;

b. The technology employed and the trends in R&D ;

c. Performance and Reliability ;

d. Vulnerabilities and limitations ;

e. The nature of counter measures which will be effective against weapon systems ;

f. War modes (WARM).

21090. In providing protection for the emissions listed, consideration must also be given to the security of any communications associated with their testing, servicing and operation, in accordance with **Chapter 23**.

21091. The underlying nature of waveform information content covered by ELSEC is as follows:

a. It is not communications information ;

b. It cannot be protected by Cryptographic Security ;

c. It is intended to be emitted at an authorised time ;

d. Once emitted it is assumed to be compromised and therefore no longer protectively marked.

Responsibilities

21092. Overall responsibility for assessing the ELSEC threat, vulnerability, and risk, lies with the MOD ELSEC Authority, InfoSy(Tech), on the staff of the Departmental Security Officer (DSO), and is implemented through the security chain of command.

21093. Responsibility for the selection of countermeasures for individual systems lies with Project Managers and or System Operating Authorities (SOA), but the individual threat assessment process is a matter purely for the security authority.

21094. In addition to the DSO, the National Technical Authority (CESG), and security / project management staffs, a number of roles are identified within MOD as having specific ELSEC responsibilities.

21095. **MOD ELSEC Technical Authority**, or their delegated representatives, are responsible for endorsing the implementation of an installation against ELSEC criteria. The task of MOD ELSEC Technical Authority (META) falls to the ELSEC Team within the EMC Division of the Army CIS Services Group at Blandford Camp.

21096. **WESSCOM** is a MOD committee, chaired by the MOD ELSEC Technical Authority, with representation from CESG, Security staffs and interested MOD TLBs to co-ordinate all aspects of ELSEC within MOD. It is accountable through InfoSy(Tech) to the Infosec Policy Review Group (IPRG) for its security responsibilities, and through EC(CCII)IOCM to the Defensive Information Operations (DIO) Capability Working Group (CWG) for Equipment Program (EP) responsibilities.

21097. The identification and measurement of electronic emissions is the task of specialist teams, which may be provided by the MOD or external agencies, such as CESG. Security staffs are to be consulted on the frequency of ELSEC On-Site Testing and are to make the necessary arrangements for inspection teams to visit locations/Units.

21098. **Project ELSEC Control Officers (PECO)**. Project Officers should be aware of the possibility of ELSEC affecting any project for which they are responsible. If necessary, Project Officers and Establishments should consider appointing a project ELSEC Control Officer (PECO); one of whose main responsibilities will be configuration control. Guidance on this topic, documentation and training is available through META.

21099. **Defence Intelligence Staffs (DIS).** The DIS is responsible for production of information relating to the current ELSEC Threat, which is then disseminated through DDefSy.

Risk Assessment

21100. A risk assessment is to be carried out early in the planning stages of a project in order to minimise any subsequent impact on design and cost caused by ELSEC considerations. A similar exercise will need to be conducted when modifications to existing equipment are proposed.

21101. The risk assessment compromises a review of the asset value, the generic and local threats, and the vulnerabilities, as is common throughout security.

21102. **Information Value** The sensitivity of an emission may be gauged from the classification assigned to the project.

a. RESTRICTED : Intercept and exploitation would be undesirable ;

b. CONFIDENTIAL : Intercept and exploitation would be dangerous ;

c. SECRET : Intercept and analysis would cause serious injury ;

d. TOP SECRET : Intercept and exploitation would normally cause exceptionally grave danger.

21103. **Threat** Several adversaries have demonstrated a sophisticated capability to exploit ELSEC vulnerabilities, and a willingness to conduct operations against facilities in their own countries or in countries where they can operate with some degree of freedom.

21104. However, ELSEC attacks are expensive in resources, difficult to mount, and unpredictable in outcome. They are therefore likely to be attempted only where all the following circumstances are met:

a. Other methods of intelligence gathering are impractical ;

b. An attack is practical (i.e. the attacker can acquire a position close enough to the radiating equipment and from which he can operate undetected over an extended period).

21105. The general ELSEC Threat to MOD facilities and equipment is provided by the Intelligence Cell within the DDefSy Joint Security Co-ordination Centre (JSyCC) as part of the regular Information Security Threat Summaries (ISTS) which are issued to defence Principal Security Advisors (PSyA) and to META. This is based upon the Annual Threat Assessment (ATA) as prepared by the Security Service and published with the endorsement of the Cabinet Office Committee on Security (SO), with the ISTS being updated from subsequent information from DIS.

21106. In addition to the ISTS, DIS issues specific warnings by formal signal message of any short-term changes to the ELINT Threat environment, such as the presence of known collection platforms (typically AGIs) within UK territorial waters.

21107. **Vulnerabilities** The likelihood, or risk, of a successful attack will depend on the extent of the perceived threat to an installation, together with the ELSEC vulnerabilities of the equipment or system involved (i.e. its propensity to radiate).

21108. The ELSEC Risk is articulated at two levels :

a. Compromise from intentional emissions caused by the normal operation of the system, with little or no measures taken to absorb its radio frequency energy output ;

b. Compromise from unintentional emissions, e.g. system in standby mode connected to a dummy load.

21109. Unintentional emissions can vary across a wide range of characteristics :

a. Compromising emanation levels near the TEMPEST limits ;

b. Much higher emanation levels associated with, for example, operation at full power into a faulty radio frequency absorbing system.

21110. Within the current risk environment, no distinction is currently considered as required between the types of unintentional emissions, and therefore the following table can be used to assess the overall ELSEC profile for a system :

Characteristic of compromising emission	Assessed Risk of Compromise (1 Apr 2001)			
	UK inland areas (more than 5km from any estuary, port or coastline)	**UK areas within 5km from any estuary, port or coastline**	**Inland areas of defence Allies (more than 5km from any estuary, port or coastline)**	**Elsewhere**
Unattenuated intentional emissions	Level 5 (Very Low)	Level 4 (Moderate)	Level 3 (Significant)	Level 2 (High)
Unintentional emissions	Level 6 (Negligible)	Level 5 (Very Low)	Level 4 (Moderate)	Level 3 (Significant)

Countermeasures

21111. The detail and amount of effort required for protection of both intentional and unintentional emissions of each system are to be assessed by considering the following key factors :

a. Purpose and sensitivity of emission ;

b. Risk of compromise of emission in its specific environment.

21112. The following baseline countermeasures can be assumed to required in all cases, be it for the development, production or maintenance stages of a system's lifecycle.

21113. Careful planning of tests and trials :

a. Avoidance of forewarning of tests and trials ;

b. Variation of times of day and, where possible, of intervals between tests and trials ;

c. Reduction to the essential minimum of:

(i) The time during which the equipment operates ;

(ii) The power need ;

(iii) The combination in one test or trial of different modes of operation of one type of equipment.

d. Receipt and review of the DIS ELINT warning messages for any short-term environmental issues.

21114. Enforcement of good OpSec discipline during trials, including ComSec and TranSec precautions as necessary. This will involve at least :

a. Pre-planning of essential messages ;

b. Avoidance of discussion over unprotected means of the results of any trial.

21115. Careful safeguarding of telemetry records and channel allocations; the latter being varied as often as practicable during a series of trials.

21116. For higher risk scenarios, additional measures may be required, and META should be approached for detailed advice.

ELSEC Control Plan (ECP)

21117. The PECO is to ensure that no unauthorized changes are made to any system which will affect the requirement for ELSEC countermeasure. The basis of the ELSEC control strategy is the ELSEC Control Plan (TCP), which the PECO is to devise, implement and maintain.

21118. The ECP is to contain the system specific details of any countermeasures required, and must be endorsed by META before any tests or trials are commenced.

Compliance Checking

21119. Where a Risk Assessment so indicates, an ELSEC On-Site Test (EOST) may be required. Further information on the principles for such activities are given at **Chapter 12,** and within Def Stan 09-3 which gives detailed information relating to acceptable emission levels and related topics.

21120. The following table provides guidance on the frequency required for EOSTs:

Risk of Compromise	System Profile		
	TOP SECRET	**SECRET**	**CONFIDENTIAL**
Level 1 (Very High)	Annually	2 yearly	5 yearly
Level 2 (High)	2 yearly	5 yearly	Not required
Level 3 (Significant)	5 yearly	Not required	
Level 4 (Moderate) Level 5 (Low) Level 6 (Negligible)	Not required		

21121. Post-test reports are forwarded to the relevant PSyAs who will specify whether any remedial action is necessary, copied to META and CESG.

Incident Handling

21122. Compromises of ELSEC should be reported, as with all other Information Security concerns, in line with the requirements of **Chapter 11**.

21123. It may be thought that once information has been disclosed there is no further need for its protection, but if a disclosure is complete, accurate and explicit, it would only free that particular item from the need for continued protection if every potentially hostile authority noted and appreciated the disclosure and believed it to be true.

21124. Disclosure could be mis-interpreted or thought to be "planted". Reliable intelligence is built by the steady accumulation of details over a period of time. Conversely reliable security results from the steady denial of every detail which might contribute to, connect with, or corroborate information from all sources, regardless of mistakes and breaches of security. A breach of security is therefore no argument for abandoning security measures.

SECTION 3 RFSEC

Radio Frequency Security (RFSEC)

21125. The measures taken to prevent interception and exploitation of those intentional electromagnetic emissions not produced specifically for communications purposes are broken down into Electronic Emission Security (ELSEC) and Radio Frequency Security (RFSEC). Although related disciplines, ELSEC is the subject of Section 2, and RFSEC is covered in this Section.

21126. The purpose of RFSEC is to protect those RF emission characteristics that attract a protective marking of RESTRICTED, or whose publicity is otherwise regarded as not desirable, but which does not require the fuller protection of ELSEC. A knowledge of such characteristics could be useful to a hostile group or country in an operational environment, and RFSEC is therefore also closely related to OpSec and EmSec.

Overview

21127. The interception of Radio Frequency (RF) transmissions of every type is an attractive and profitable source of intelligence, in particular because the large theoretical propagation distances as detailed at **Chapter 26** means it can in principle be undertaken from the safety of home territory; international air space; or the high seas; and from foreign diplomatic and trade premises, or during other activities, in the United Kingdom.

21128. RF interception can reveal information relating certain aspects of the electronic techniques employed in the equipment; the extent and preparedness of the country's defences, and the capacity of its industrial resources which is otherwise protected by physical, personal and CIS security measures.

21129. The aim of RFSEC practices is to minimise, as far as possible, the risk of compromise of emission information that would in itself be protectively marked, by limiting the opportunities for its interception by any hostile group or country. Total denial is impracticable in most cases without seriously impeding the progress of a project through its developmental stages and more so when operational. Emitters must emit; but the security aim must be to assess the risk and implications of compromise by interception and then to apply protective measures commensurate with protective marking, the characteristics of the emission, and the local conditions.

21130. The protective marking associated with information obtainable from interception of non-communications electronic emissions, is generally considered to be higher in the early stages of research and development. Although it may not be practicable to maintain the same degree of security from the beginning of development of equipment to the in-service date and beyond, continuation of security is essential.

21131. The technical analysis of such emissions can provide data which may also allow development of similar equipment or systems, but also effective electronic countermands (ECM). These may involve sophisticated deception and decoy techniques or jamming. Indeed successful interception and analysis could allow the development and deployment of countermeasures to coincide with the operational use of the target signals.

21132. The intercept of only seconds of a complex signal can provide vital information as to its purpose, modes and technical characteristics. Whereas a high signal level is necessary for the type of detailed analysis against which ELSEC countermeasures are deployed, low signal level can also be beneficial interceptor and may help target a subsequent attempt at interception with greater resources.

21133. A variety of system types exist for which RF emissions will need to be considered for RFSEC, including:

a. Radars ;

b. Radio Transmitters including Beacons;

c. Any receiver equipments utilising a Local Oscillator (LO) including Navigational aids;

d. Weapon Electronic Systems ;

e. Targets and Decoys.

21134. Although the interception of occasional individual emissions is of relatively small importance in terms of ELSEC, RFSEC protection is needed to restrict the amount of information revealed concerning:

a. Intended emission frequency band(s) of system ;

b. Collateral emission frequency band(s) of system, especially those associated with LO and similar effects ;

c. Locations of emitters, research establishments and facilities used for testing systems and part systems ;

21135. In providing protection for the emissions listed, consideration must also be given to the security of any communications associated with their testing, servicing and operation, in accordance with **Chapter 23**.

Responsibilities

21136. Overall responsibility for assessing the RFSEC threat, vulnerability, and risk, lies with the MOD RFSEC Authority, InfoSy(Tech), on the staff of the Departmental Security Officer (DSO), and is implemented through the security chain of command.

21137. Responsibility for the selection of countermeasures for individual systems lies with Project Managers and/or System Operating Authorities (SOA).

Risk Assessment

21138. A risk assessment is to be carried out early in the planning stages of a project in order to minimise any subsequent impact on design and cost caused by RFSEC considerations. A similar exercise will need to be conducted when modifications to existing equipment are proposed.

21139. The risk assessment compromises a review of the asset value, the generic and local threats, and the vulnerabilities, as is common throughout security.

21140. **Information Value** The sensitivity of an emission may be gauged from the classification assigned to the project.

a. RESTRICTED : Intercept and exploitation would be undesirable ;

b. CONFIDENTIAL : Intercept and exploitation would be dangerous ;

c. SECRET : Intercept and analysis would cause serious injury ;

d. TOP SECRET : Intercept and exploitation would normally cause exceptionally grave danger.

21141. **Threat** The simple interception of signals does not require the technically sophisticated facilities needed for analysis of the types of waveform information which ELSEC seeks to protect, and thus many potential adversaries, including terrorist groups, can easily acquire the capability to exploit RFSEC vulnerabilities.

21142. However, RFSEC attacks can be expensive in manpower resources, and are inherently unpredictable in outcome. They are therefore likely to be attempted only where the attacker can acquire a position close enough to the radiating equipment and from which he can operate undetected over an extended period.

21143. The general RFSEC Threat to MOD facilities and equipment is provided by the Intelligence Cell within the DDefSy Joint Security Co-ordination Centre (JSyCC Int) as part of the regular Information Security Threat Summaries (ISTS) which are issued to Principal Security Advisors (PSyA) in MOD. This is based upon the Annual

Threat Assessment (ATA) as prepared by the Security Service and published with the endorsement of the Cabinet Office Committee on Security (SO), with the ISTS being updated from subsequent information from DIS.

21144. In addition to the ISTS, DIS issues specific warnings by formal signal message of any short-term changes to the ELINT Threat environment, such as the presence of known collection platforms (typically AGIs) within UK territorial waters.

21145. **Vulnerabilities** The likelihood, or risk, of a successful attack will depend on the extent of the perceived threat to an installation, together with the RFSEC vulnerabilities of the equipment or system involved (i.e. its propensity to radiate). The following table can be used to assess the overall RFSEC profile for a system :

Assessed Risk of Compromise (1 Apr 2001)			
UK mainland areas (more than 5km from any estuary, port or coastline)	**UK areas within 5km from any estuary, port or coastline, and Northern Ireland**	**Inland areas of defence Allies (more than 5km from any estuary, port or coastline)**	**Elsewhere**
Level 5 (Very Low)	Level 4 (Moderate)	Level 3 (Significant)	Level 2 (High)

Countermeasures

21146. The detail and amount of effort required for protection of both intentional and unintentional emissions of each system are to be assessed by considering the following key factors :

a. Purpose and sensitivity of emission ;

b. Risk of compromise of emission in its specific environment.

21147. The following baseline countermeasures can be assumed to required in all cases, be it for the development, production or maintenance stages of a system's lifecycle.

21148. Careful planning of tests and trials :

a. Avoidance of forewarning of tests and trials ;

b. Variation of times of day and, where possible, of intervals between tests and trials ;

c. Reduction to the essential minimum of:

(i) The time during which the equipment operates ;

(ii) The power need ;

(iii) The combination in one test or trial of different modes of operation of one type of equipment.

d. Receipt and review of the DIS ELINT warning messages for any short-term environmental issues.

21149. Enforcement of good OpSec discipline during trials, including ComSec and TranSec precautions as necessary. This will involve at least :

a. Pre-planning of essential messages ;

b. Avoidance of discussion over unprotected means of the results of any trial.

21150. Careful safeguarding of telemetry records and channel allocations; the latter being varied as often as practicable during a series of trials.

21151. For higher risk scenarios, additional measures may be required, and InfoSy(Tech) should be approached for detailed advice.

Incident Handling

21152. Compromises of RFSEC should be reported, as with all other Information Security concerns, in line with the requirements of **Chapter 11**.

21153. It may be thought that once information has been disclosed there is no further need for its protection, but if a disclosure is complete, accurate and explicit, it would only free that particular item from the need for continued protection if every potentially hostile authority noted and appreciated the disclosure and believed it to be true.

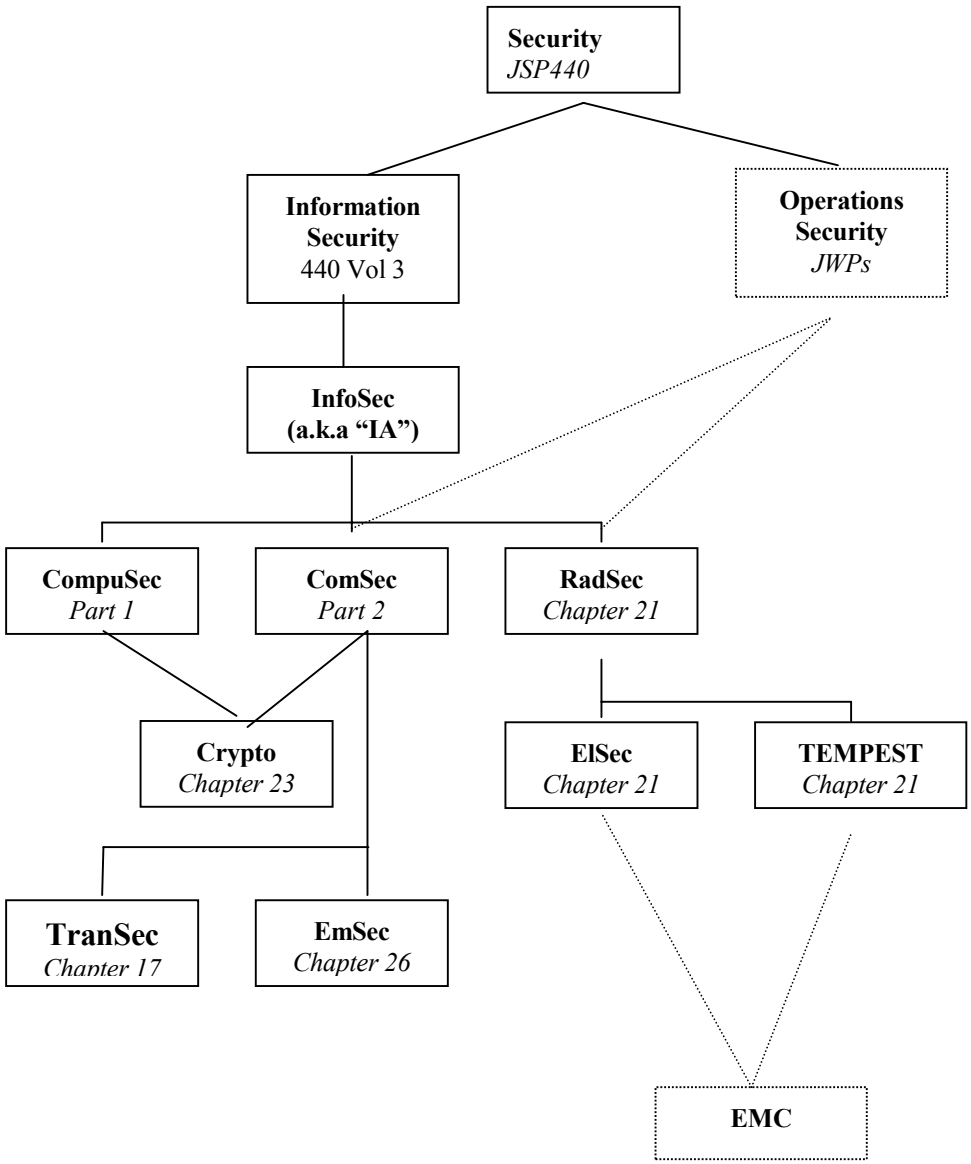
21154. Disclosure could be mis-interpreted or thought to be “planted”. Reliable intelligence is built by the steady accumulation of details over a period of time. Conversely reliable security results from the steady denial of every detail which might contribute to, connect with, or corroborate information from all sources, regardless of mistakes and breaches of security. A breach of security is therefore no argument for abandoning security measures.

ANNEX A TO

CHAPTER 21

RELATIONSHIP OF DISCIPLINES

The following diagram attempts to provide a high level illustration of the inter-relationships between disciplines in the context of RadSec.



Fuller details of the non-technical aspects of Information Security are given at **Chapter 1**.

This page intentionally left blank.

ANNEX B TO

CHAPTER 21

CO-ORDINATING INSTALLATION DESIGN AUTHORITY

Initial Points Of Contact

AREA	BRANCH	ADDRESS	TELEPHONE
MOD HQ, Centre, List X and DPA	DCSA CIDA	Minerva House	5353 MIN Fax 5359 MIN
DSTL SCIDA	IT Security Administrator	Room G304, DSTL Malvern	01684 894531 Fax 01684 896070
Met Office SCIDA	CIDA Manager	Beaufort Park	01344 855616 Fax 01344 855878
Royal Navy	DCSA INF 4	Forth Southwick	5428 FW Fax 5444 FW
Army	CPD, Army CIS Engineering Group	Blandford Camp	5277 BLN Fax 5461 BLN
Royal Air Force	DCSA DEI DS6	RAF Henlow	7886 HEN Fax 7687 HEN

This page intentionally left blank.

ANNEX C TO

CHAPTER 21

TEMPEST MINIMUM STANDARDS

TEMPEST Countermeasures and Installation Standards

Equipment and systems used to process information protectively marked CONFIDENTIAL and above

INSPECTABLE SPACE / TEMPEST THREAT LEVEL	Less than 20 metres [1]	Greater than 20 metres but Less than 100 Metres	Greater than 100 metres
Level 1 (Very High)	**Consult your TEMPEST authority**		
Level 2 (High)	**AMSG-720 equipments[2], installed to AMS719**	**AMSG-788 or Military EMC[3] equipments[2], installed to AMS719**	**AMSG-784 or Military EMC[3] equipments[2], installed to AMS719**
Level 3 (Significant)	**AMSG-788 or Military EMC[3] equipments[2], installed to AMS719**	**AMSG-784 or Military EMC[3] equipments[2], installed to AMS719**	**Civil EMC equipments, installed to JSP480[4]**
Level 4 (Moderate)	**AMSG-784 or Military EMC[3] equipments[2], installed to AMS719**	**Civil EMC equipments, installed to JSP480[4]**	
Level 5 (Low)	**Civil EMC equipments, installed to JSP480[4]**		
Level 6 (Negligible)	**Civil EMC equipments, installed to JSP480[4]**		
Note 1	Inspectable Space less than 8 metres, consult both the PSyA and CIDA.		
Note 2	Civil EMC for military deployments to new locations for the first month.		
Note 3	Military EMC is DEF STAN 59-41 or US equivalent MIL-STD-461		
Note 4	All equipment built to AMSG-784 or higher, cryptographic equipments, transmitter equipments and their associated cabling, and approved or protected circuits transiting MOD site boundaries shall be installed in accordance with AMSG-719F		

Equipment and systems used to process UNCLASSIFIED and/or RESTRICTED information

In all cases, Civil EMC equipment required installed in accordance with JSP 480

ANNEX D TO

CHAPTER 21

TEMPEST CONTROL OFFICER (TCO)

Responsibilities

1. The TEMPEST Control Officer (TCO) is responsible for ensuring that all CIS facilities processing data protectively marked CONFIDENTIAL and above are properly installed in accordance with JSP 440 Chapter 21 and Sector TEMPEST Authority directives. He is to ensure that only authorized changes are made to CIS facilities that are subject to TEMPEST Control or countermeasures and is to devise, implement and maintain a TEMPEST Control Plan (TCP)

2. Enforcement of installation standards and TEMPEST countermeasures on operations requires personnel with the appropriate engineering skills, authority, responsibility and training. This Annex details the role of the TCO for both static and deployed locations. The Terms of Reference for a TCO are at Appendix 1. The TCO role is complementary to the ITSO role and both are required to gain accreditation.

Accountability

3. The TCO is responsible to the senior UK commander at his location for all aspects of his task. A Static Site TCO will normally be superseded by the appointment of a SCIDA (who may be the same person) for installations that become permanent.

Deployment TCO

4. During a deployment, installation security may be achieved by filtering and interlinking vehicles, cabins or discrete equipment in an approved manner. However, deployments are now commonly made by multi-national as ad hoc HQs, frequently with commercial-of-the-shelf equipment using host-nation infrastructure.

5. The UK force commander of a deployment away from CIDA planned or established sites is responsible for the security of UK national information throughout the deployment by enforcing the relevant sections of security policies including those relating to installation practice. The enforcement of TEMPEST installation standards needs to have a focus of accountability for the whole site. Therefore, a Deployment TCO is to be appointed for all sites with UK national IT

systems processing protectively marked information where the occupancy exceeds, or is expected to exceed, one month.

6. The TCO must work closely with the designated Sector TEMPEST Authority and the CIDA, if applicable. The TCO should be the Force CIS Officer (FCISO). This individual is to be clearly nominated and given sufficient authority by the UK force commander to carry out his duties.

Training

7. The TCO must be experienced and trained in general installation and TEMPEST matters. Additionally, a Deployment TCO is required to provide TEMPEST advice in a role where he may be isolated from support for extended periods of time.

8. The TCO should have a basic understanding of both fixed-site and mobile installation design criteria, TEMPEST phenomena and related electromagnetic vulnerabilities, cost-effective countermeasures, documentation and support services, practical problems encountered when applying theoretical principles, copper and fibre usage, connection and isolation.

9. TCO training is provided under Sector Security Authority arrangements and is typically 2 days in duration. CESG provide a 2-day Background and Installation course available for all personnel; additionally, the Army provides TEMPEST training on the Foreman of Signals (FofS) Course and the TOT/FofS Refresher Course, and the RAF provides a 2 day Seminar at 591 SU, RAF Digby.

ANNEX E TO

CHAPTER 21

TEMPEST CONTROL PLAN (TCP)

Introduction

1. The TCO will maintain a register of all installations processing protectively marked information. The purpose of this Annex is to state the minimum required contents of the TEMPEST Control Plan.

Tempest Control Plan Format

2. The TCP is to include the following elements:

a. Preliminary pages containing:

(1) Introduction.
(2) List of Contents.
(3) Appointments (ie TCO, Deputy TCO, LCOs, SyO etc).

b. Administration section containing:

(1) TEMPEST Threat Assessment/TEMPEST Certificates.
(2) TCA/TVI applications.
(3) Outstanding TEMPEST problems.
(4) Restrictions in force.
(5) List of CIDA/IDA.
(6) Terms of Reference for TCO, Deputy TCO, LCOs etc.
(7) Copies of local TEMPEST orders/instructions.

c. Register of assets covering: (See Appendix 1)

(1) RED systems locally registered by the TCCO.
(2) RED systems having full TEMPEST certification. (See note 1)

d. Record of regular configuration inspections for TEMPEST certified systems and annual checks for locally registered systems.

e. Historic information. (e.g. removed equipment which may appear on other systems' configuration diagrams)

Note:

Each TEMPEST certified system should have the following documentation:

TCA/TVI application and report.
TEMPEST Certificate.
Configuration Diagrams authorised by Sector TEMPEST Authority.

APPENDIX 1 TO ANNEX E TO CHAPTER 21

PROTECTIVELY MARKED CIS RECORD CARD

TCP Reference:

Distribution: TCO one copy (for retention in TCP)

PART 1. LOCATION DETAILS

1. User Formation/Unit.
2. Location, Building and Room No(s) containing terminal equipment.
3. CIDA responsible for room containing equipment.
4. Location security authority responsible for room containing equipment.
5. Location engineering authority responsible for room containing equipment.

PART 2 PROTECTIVELY MARKED CIS

Local Registration No	System/ Installation Name	Location	Equipment Details	TEMPEST Certificate No	Remarks

This page intentionally left blank

CONTROLLED CIRCUITS

This page intentionally left blank.

CHAPTER 22

CONTROLLED CIRCUITS

Definitions

2201. A "Controlled Circuit" is any Defence communications link that has been authorized for the transmission of Official Information.

2202. A Controlled Circuit consists of a land line (either fibre optic or wire), the associated terminal and any intermediate equipments, and applies to all communications circuits whether by dedicated point to point links or those forming part of a network such as a Local Area Network (LAN) of a computer installation.

2203. A “Protected Circuit” is a Controlled Circuit authorized for the unencrypted transmission of Official Information protectively marked RESTRICTED outside of a controlled GSE.

2204. An “Approved Circuit” is a Controlled Circuit authorized for the unencrypted transmission of Official Information protectively marked CONFIDENTIAL or above, which would otherwise attract the use of High Grade (HG) encryption systems, as laid down at **Chapter 23**.

Approval Of Circuits

2205. All Controlled Circuits must be authorised by a Coordinating Installation Design Authority (CIDA), or their nominated representative. All data circuits within an MOD controlled GSE are to be Controlled Circuits.

2206. Where Controlled Circuits are required to carry Official Information protectively marked RESTRICTED unencrypted outside of a MOD GSE controlled area these must be made into Protected Circuits, which incorporate some measure of additional protection.

2207. Where Controlled Circuits are required to carry Official Information protectively marked CONFIDENTIAL or above, these must be made into Approved Circuits, which are defined as ones installed in such a way that interception or compromise is made difficult, and/or easy to detect.

2208. Where a Protected or Approved Circuit is required, additional approval must be obtained from the Principal Security Advisor(s) (PSyA) responsible for the affected establishment(s).

2209. Where a system requires the use of Protected or Approved Circuits, system sponsors/project officers are to seek approval in principle from both the PSyA(s) and Accreditors before entering into commitments which depend on Approved Circuits being available.

2210. Controlled Circuit policy is intended to provide appropriate electromagnetic and/or physical safeguards to meet the specific threats and vulnerabilities of the installation being considered, and any other installations in the vicinity.

2211. In the case of Protected or Approved Circuits, this will include measures so as to minimise the risk of interception.. Approval procedures are to take into account each specific component of a circuit, including line, terminal, and intermediate equipment.

2212. Any Circuit whose physical installation is such that interception is made relatively simple, and/or is difficult to detect, may only carry RESTRICTED and UNCLASSIFIED information.

2213. Wireless networking technologies, using Radio Frequency (RF) or Infrared (IR) carriers, are normally only permitted for carriage of UNCLASSIFIED information. Exceptionally, RESTRICTED information may utilise wireless technologies, but only in cases where both the PSyA and CIDA have approved the specific implementation.

Approval Procedures

2214. Applications for approval of circuits are to be made by the Installation Design Authority (IDA), as the technical authority, via the security chain of command. For all circuits, confirmation is required that the following criteria have been met:

a. Terminal equipment is protected to prevent unauthorized persons gaining access to protectively marked information. This may be achieved by access controls or removing storage components, such as removable disks, when the equipment is not in use. Where this is not possible, terminal equipment is to be given the same protection as the highest protective marking of material processed.

b. Intermediate equipment such as junction boxes, patching panels, wiring centres etc, whether active or passive, are to be physically protected to ensure that only appropriately cleared persons in the performance of their duties can gain access.

c. All Controlled Circuits are to meet the National and Departmental TEMPEST regulations laid down in **Chapter 21**.

2215. For Protected Circuits, confirmation is also required the area in which the circuits are contained is able to be adequately supervised by establishment, with

supporting measures to minimise the risk of tampering which must be approved by the CIDA.

2216. Modifications to Controlled, Protected or Approved Circuits, or changes in environmental factors which may affect the approved status are to be notified to the CIDA, and, in the case of Approved Circuits, also to the approving authority.

Physical Protection of Approved Circuits

2217. For Approved Circuits, confirmation is required the area in which the circuits are contained is to be directly under the physical control of the establishment.

2218. Circuits which are contained entirely within a building which meets the physical security requirements of a minimum of 6 points aggregated from the Guard/IDS/Entry Control sections of the assessment matrix in **JSP 440 Volume 1 Chapter 5** and where the possibility of undetected interception is negligible, may carry information up to and including SECRET without additional physical protection to the line element. On exit from such buildings, circuits approved for SECRET and below are to be contained in secure ducting. Where practicable, manhole covers provided to permit access to the cabling, are to be secured by class 3 security padlocks. The keys to the padlocks are to be handled as security keys. Where this is not practicable alternative physical security measures, as advised by the security authority, are to be taken.

2219. Intermediate equipment forming part of a system featuring approved circuits is to be protected so as to deny unauthorised access. This may be by the use of sealed boxes, lockable containers or rooms or areas to which specific security measures have been taken to protect the contents. The standard of security to be achieved is commensurate with the protective marking of information to be protected. Protectively marked equipment is to be secured to the level of its marking; UNCLASSIFIED equipment is to be protected to an equivalent standard that is given to RESTRICTED material. When assessing the physical security requirements for intermediate equipment, each location will be considered independently.

2220. Whilst the above is the minimum standard for physical protection there may be occasions when it is considered necessary to apply additional measures such as sealing of conduit/trunking in which circuits are installed to make the detection of intrusion easier. Where this is contemplated, system security officers/IDAs should seek advice from the Sector Security Staffs.

2221. Circuits in buildings which do not meet the physical security standards detailed at para 2218 may be considered for approval for SECRET and below providing additional safeguards are taken to provide protection to all elements of the circuit including the line, commensurate with the physical security protection provided by the building or establishment. The standards of protection will be advised by PSyAs on a

case by case basis. Measures taken must also be designed to reveal any signs of tampering or intrusion.

Use of Fibre-Optic Cables

2222. Whilst not totally immune from interception, fibre-optic cables provide a greater degree of security than other media such as copper wire. Where it is intended to seek approved circuit status, project officers should consider the use of fibre optic cables in preference to metallic conductors.

2223. Where fibre-optic cables are to be installed, the CIDA will request a performance test of each fibre on initial installation, and the results of such tests should be archived to allow future comparison if required.

2224. Splices or connections in fibre-optic cables increase their vulnerability to interception although this is reduced by permanent splicing such as fusion. Where it is necessary to splice fibre-optic cables, the fibre optic connector or splice, including fusion splicing, is to be protected in accordance with para 2219 above.

Use of Wireless Networking Technologies

2225. Wireless Local Area Networks (LANs) typically use either a specialised form of Radio Frequency (RF) transmission as described at **Chapter 26**, or, less commonly, infra-red (IR). RF wireless LANs typically used is usually direct sequence spread-spectrum techniques, which is intended to provide a good quality, interference resistant, signal. IR wireless LANs are subject to a very rapid signal degradation beyond their intended operating environment.

2226. Where a requirement is identified to use wireless LANs within a MOD controlled building, the following constraints will apply to all installations :

a. All installations using wireless networking must be within the UK mainland ;

b. Where RF technologies are employed, both a CIDA review of the building and the power levels of the equipments, to address TEMPEST concerns laid down at **Chapter 21**, will be required.

2227. If the requirement is for use with Protectively Marked information, unless CESG approved encryption is to be used, where the maximum level will be that laid down in **Chapter 23**, the maximum permitted level will be RESTRICTED, and this will be subject to the following additional constraints :

a. The PSyA will need to review the environment, and in particular the proximity and nature of any neighbours, before deciding whether or not wireless networking can be permitted ;

b. Only IR networking technologies should normally be employed.

Control Of Patching Facilities

2228. If Controlled, Approved and/or Protected Circuits of differing protective marking levels are present within the same patching facility or junction box, the layout must preclude any interconnection or cross-patching between Circuits of dis-similar levels.

2229. In the exceptional case of the installation of either multi-security level (MSL) or one-way devices that bridge between protective marking levels, in addition to any Accreditation requirement accruing from **Chapter 6** in respect of the software or hardware mechanisms implemented to maintain separation, it is also important that for TEMPEST reasons, as detailed at **Chapter 21**, Electromagnetic separation is provided across the interface, which will normally necessitate at least one of the controlled circuits forming the signal path to be implemented in Fibre-optic cable.

Configuration Control of Controlled Circuits

2230. All circuits forming an infrastructure are to be accounted for. Each fibre or wire circuit is to be clearly and uniquely identified at each end of the cable and along its length as appropriate.

2231. Where metallic conductors or fibre-optic cables are allocated to a specific system, each line or fibre-optic cable is to be terminated. The system security officer is responsible for ensuring that a record is kept of each cable and its termination. This information is also to be supplied to the CIDA for the building or site.

2232. Where fibre-optic cables are not allocated to a specific system, these may remain unterminated but are to be under the control of the CIDA. A record of each unterminated fibre is to be notified to the CIDA. Initial allocation of fibres is to be dictated by CIDA.

2233. Changes to configuration, where fibres are transferred from one system to another, are to be agreed by both system security officers and co-ordinated by the CIDA.

2234. All unterminated fibres should be physically inspected and accounted for annually.

System Security Documentation

2235. The Security Policy Documentation (SPD) that is produce for the affected systems in accordance with **Chapter 3** should reflect the provision of Approved

Circuits. The SPD should address the physical safeguards to be applied, maintenance and inspection to ensure the continued integrity of the circuits.

2236. The Installation and Commissioning Security Instructions (ICSyI) and Technical Operation and Maintenance Commissioning Security Instructions (TOMSyI) for communications/computer systems utilising Protected and Approved Circuits should address access procedures for all equipments that form part of such circuits, such as patching panels, modems and multiplexers.

Maintenance

2237. Maintenance of Controlled circuits is only to be carried out by, or under the direct supervision of technically qualified persons, holding security clearance commensurate with the protective marking of material for which the circuit has been approved.

Inspections

2238. Approved circuits are to be inspected by or under the direction of the System Security Officer appointed under the OSMP. Inspections are to be carried out at regular intervals as detailed in the OSMP. Inspections should concentrate on areas where the approved circuit is most vulnerable ie junction boxes, roof and ceiling voids where the cable route is out of sight. The inspection is intended to reveal whether attempts have been made to intercept transmissions by the attachment of devices or unauthorized additional cables. Special attention should be paid to unaccountable cables diverting from the authorized route. A guide to points to be addressed during inspections is contained in Annex A; System Security Officers may seek further guidance from PSyAs.

Approval for Top Secret

2239. Where a department/organisation considers there is a requirement to pass TOP SECRET or Compartmented (Codeword) information without encryption, advice should be sought from InfoSy(Tech) via the Accreditors.

ANNEX A TO

CHAPTER 22

INSPECTION OF APPROVED CIRCUITS

1. Whilst not exhaustive, the following is provided as a guide and "aide memoire" to persons responsible for carrying out inspections of approved circuits.

2. The following should be investigated:

(a) Unaccountable wiring or equipment attached to or leaving terminal equipment.

(b) The use of "T" or "Y" connectors on fibre optic cables.

(c) Lines leading to uncontrolled areas.

(d) Splices or bridges in jumper runs.

(e) Unaccountable wiring or equipment attached to intermediate equipment such as modems multiplexers etc.

(f) Unaccountable wiring or equipment connected to junction boxes.

(g) Monitoring devices such as amplifiers, headphones or automatic recorders.

(h) Small capacitors and/or resistors on terminal blocks which may be used for high impedance bridging.

(j) Equipment attached to fibre-optic cables along the route of the cables.

(k) Unaccountable lines connected to underground cables at jointing sleeves in manholes and cable chambers.

(i) Confirmation of "as fitted" documentation.

This page intentionally left blank.

CRYPTOGRAPHIC SYSTEMS

CHAPTER 23

CRYPTOGRAPHIC SYSTEMS

Purposes of Cryptography

2301. Cryptography is defined as being the art or science concerning the principles, means and methods for rendering plain text unintelligible, and for converting encrypted messages into an intelligible form.

2302. This definition basically refers to the use of Encryption / Decryption for Confidentiality, but it is worth noting that cryptographic techniques are also used for Authentication (e.g. Digital Signatures) and Integrity (e.g. Cryptographic Checksums and Message Digests).

2303. Cryptography is implemented in one of two distinct manners :

a. Symmetric cryptography, where it is essential that all the cryptographic key variables are private between parties involved in the particular community. This is sometimes referred to as private key cryptography ;

b. Asymmetric cryptography, where there are 2 types of cryptographic key variables, a private key for a particular user or community, and a public key which can be freely published. This is usually referred to as Public Key Cryptography (PKC).

2304. Most HMG approved encryption systems currently deployed are based upon symmetric cryptography, but there are a growing number of asymmetric systems being developed.

2305. It should be remembered that even when the content of a message is encrypted and cannot be read, a determined long-term attacker can often gain valuable information by analysing the flow of information between parties on a communications network. This can reveal chains of command or links between organisations and their locations. Increased activity can indicate reactions to an event or interest in a particular incident. Traffic flow security (TFS) techniques can be applied to link encryption devices to make it appear that the link is constantly active by making the genuine traffic indistinguishable.

Specialist ComSec Publications

2306. This Chapter is only intended to give an overview of the Security requirements relating to Cryptographic Systems, and to provide a readily accessible source of

guidance on the use of certain Cryptographic Systems that due to their widespread deployment are not solely constrained to use by Authorised Cryptographic personnel. Fuller details regarding cryptographic material, definitions, marking, handling and Authorization are given in the relevant specialist ComSec publications, details of which can be obtained by authorised personnel from either the Defence COMSEC Authority (InfoSy(Tech) within DDefSy) or the Defence COMSEC Operating Authority (IA branch within DCSA).

Definition

2307. Although full details are given in the relevant specialist ComSec publications, the following definitions are offered to allow initial discussions to take place.

2308. A Cryptographic system is defined as a manual or automated method for rendering plain text unintelligible, and for converting encrypted messages into an intelligible form.

2309. Cryptographic equipment is defined as any equipment whose purpose is to provide protection within communications systems by rendering any information being passed over the system unintelligible and unrecognizable until it reaches the intended recipient. Cryptographic equipment used for the security of HMG protectively marked information must be approved by CESG.

2310. Cryptomaterial is defined as any material pertaining to a cryptosystem or containing information relating to the operation and protection of cryptosystems.

2311. Cryptographic Keymaterial, often referred to as Key Variables or KV, or historically as cryptovariables (CV), is defined as the specific key setting for a given period.

2312. Cryptographic Authorisation is defined as the mandatory approval and education procedures required before personnel prior are granted direct access to cryptomaterial.

2313. Cryptomaterial may attract an additional restrictive markings (e.g. CRYPTO) in addition to its protective marking, to indicate the need to limit access and apply extra controls.

Grades of Cryptography

2314. Cryptographic systems and equipment are graded according to the level of protection they provide. The grade of cryptography available will be a major factor in the selection and approval for a particular purpose. The grades of cryptography authorised for use in MOD are:

a. **High Grade.** High Grade (HG) cryptography is solely provided as cryptographic equipments which have been designed in-house by CESG to provide long term security for highly sensitive information ;

b. **Enhanced Grade.** Enhanced Grade (EG) cryptography provides security for sensitive information both within and outside Great Britain, and may be implemented in either cryptographic equipments or in software, using either CESG designed algorithms, or public domain algorithms that have been approved by CESG ;

c. **Baseline Grade.** Baseline Grade (BG) cryptography offers limited protection for Official information, and will normally be found as a software implementation of Public Domain (PD) algorithms that have been approved though the CESG Assisted Product Scheme (CAPS), or in some Legacy cases by the implementation of a CESG furnished algorithm. Wherever possible, BG solutions based on PD implementations are preferred for defence use, as these will require less constraints in their handling and distribution, especially overseas.

Selection of Appropriate Cryptographic Systems

2315. In selecting the grade of cryptography required for MOD systems, the following matrix is to be used:

Protective Marking	Overall Grade of Encryption Required
TOP SECRET	High Grade (HG)
SECRET	
CONFIDENTIAL	Enhanced Grade (EG)
RESTRICTED	Baseline Grade (BG)

Note
There may be instances encountered where there is a discrepancy between the strength of the cryptographic algorithm used, and the architectural protection afforded by the system implementation.
In such case the **Overall Grade of Encryption** is determined by the **lower** of these two ratings.

2316. MOD policy differs from the guidance given in the Government Manual of Protective Security (MPS) and CESG Handbook on Cryptographic Security (BID/01/1) in that :

a. MOD does not routinely permit the protection of "short term SECRET" information (which is defined in MPS as information which is likely to have decreased to the equivalent of CONFIDENTIAL or less within one year) by Enhanced Grade (EG) cryptography. However, the MOD does recognise the concept of genuine ephemeral data, as laid down at **Chapter 1**,

and the requirements above may be varied on a case by case basis provided that the Defence ComSec Operating Authority can be satisfied that the information in question is genuinely ephemeral within the sense of this manual ;

b. MOD requires RESTRICTED material elsewhere in the UK than the mainland (e.g. Northern Ireland) to be protected by encryption whilst in transit.

2317. System sponsors are to provide Defence ComSec Operating Authority with details of their intended secure communications link/network during initial planning stages. This should include information on the community of interest/size of network, location of terminals, protective marking of information to be passed and whether any special categories of information are to be handled.

2318. For situations requiring either HG and EG cryptography, Traffic Flow Security (TFS) techniques will normally be required, and any decision not to implement such an approach must be agreed with the Defence ComSec Operating Authority. Where requirements are identified to use cryptographic equipments in a manner for which they are not explicitly approved (e.g. encrypting LOW across HIGH), specific sanction must be sought from the both the Defence ComSec Operating Authority and InfoSty(Tech).

2319. All approved cryptosystem are to be operated in accordance with the relevant Handling Instructions, which will be either in the form of a British Interdepartmental Document (BID), normally for HG systems, or a Defence Information Assurance Notice (DIAN), normally for EG and BG systems. It should be noted that completion of the CAPS approval process for EG and BG systems does not mean that either KV generation procedures or Handling Instructions will have been completed, and it is the responsibility of the Defence Infosec Product Co-ordination Group (DIPCOG), chaired by InfoSy(Tech) with representation from both the Defence ComSec Operating Authority and CESG to ensure that these steps have been completed before issuing a DIAN which will allow the use of such products in defence.

Public Key Cryptography

2320. Public Key Cryptography (PKC), and in particular the Public Key Infrastructures (PKI) needed to support any large scale implementation of PKC within Defence, is the subject of evolving policy.

2321. PKC equipments not requiring the use of any supporting PKI (e.g BID/2010 *BRENT*) may be used in Defence in accordance with the operating instructions detailed in the appropriate national and/or departmental publications.

2322. Any requirement for the use of PKI with Defence should be referred to both the MOD PKI Management Authority for advice, and must be endorsed by both the Defence ComSec Operating Authority and the Accreditator(s) before procurement action is initiated.

Operational Exigencies

2323. In extreme circumstances, an Operational Commander of not less than 2* rank may determine that there are operational imperatives for Enhanced Grade (EG) encryption to be used for the protection of "short term SECRET" information, accepting the consequential security risks. These circumstances should only be for a limited time period, for example, the duration of a specific operational mission, must be notified in writing to the Defence ComSec Operating Authority, and must only be in respect of a Communications or IT systems or Networks **wholly within** the Commander's jurisdiction. These circumstances will therefore not be permitted in a networked environment where a Commander's decision could lead to a propagation of unacceptable risk(s) to the rest of the community, or where third party controlled or released information is stored or processed on the system(s).

2324. When considering the use of Enhanced Grade (EG) encryption for the protection of short term SECRET information, if any of the following considerations apply then the use of High Grade (HG) encryption will continue to be required:

a. Communication links which are especially attractive to foreign intelligence services ;

b. Large communication networks or high volume links readily interceptible by a foreign intelligence service ;

c. Situations where the local Threat is greater than Level 4 (Moderate) and TEMPEST or tamper protection is an issue.

Approval Procedures

2325. When it has been determined that encryption is necessary the Defence ComSec Operating Authority will identify the most appropriate equipment for the purpose and give approval for the requirement. Any approval will be restricted to a particular area of operations, will limit the type of information to be passed and will only be on a case by case basis. Approval for use of cryptographic equipment will not be delegated to any other organisation.

Procurement of Crypto Equipment

2326. When the correct grade of equipment has been determined and approved, demand or procurement action, sometimes referred to as a Crypto Callout, is to be taken through appropriate cryptographic equipment sponsors. It should be noted that significant lead times may be required for some types of cryptographic equipment.

Provision of Cryptographic Keymaterial

2327. The Defence ComSec Operating Authority is responsible for the provision and management of cryptographic keymaterial for secure systems. Having been made aware of potential requirements (para 2317), the Defence ComSec Operating Authority will liase with the system sponsor to enable the appropriate type of cryptographic keymaterial to be produced. At least 3 months advance notice must be given of any requirements.

2328. TEST keymaterial will be provided to locations where cryptographic equipment is to be installed to facilitate engineering of the equipment and testing the installation. Operational keymaterial will not be authorised for issue until the installation has been certified as satisfactory by the IDA/CIDA.

2329. Cryptographic keymaterial will normally distributed through Crypto channels in accordance with established cryptographic procedures. Any variance from this approach must either be documented in the Handling Instructions for the cryptosystem in question (either a BID or a DIAN), or be specifically authorised by the Defence ComSec Operating Authority.

Provision of Cryptographic Equipment to Defence Contractors

2330. Cryptographic equipment to be provided to Defence Contractors, who must have List X status, for any purpose other than repair under an existing MOD contract, must have prior approval from the Defence Security Standards Organisation (DSSO Comsec Office), acting on behalf of DCSA. Project Sponsors or other authorities seeking this approval should provide the contract number which dictates the issue.

Handling Requirements

2331. Cryptomaterial bearing the CRYPTO marking, referred to as CRYPTO Items, require special handling and whole-life accounting procedures, and detailed guidance on the measures for CRYPTO Items is contained in BID/01/1.

2332. Other items of cryptomaterial which do not warrant CRYPTO marked handling and whole-life accounting procedures may attract specific requirements, either generically as in the case of US sources Crypto Controlled Items (CCI) or on a case-by-case basis as laid down in the relevant BID or DIAN.

Movement of Cryptographic Equipment

2333. Where cryptographic equipment protectively marked CONFIDENTIAL or above is not subject to special handling within CRYPTO channels (i.e. supplied through stores channels), it should be moved in accordance with the regulations for the movement of protectively marked equipment as detailed in **JSP 440 Volume 1**. Any

item bearing the CRYPTO marking must, of course, be moved through CRYPTO channels.

Export Control Aspects

2334. Cryptographic systems are regarded by many countries as requiring specific export controls, unless they have a symmetric key of less than 128 bits which are exempted under the terms of the *Wassenaar Arrangement*.

2335. All HG and EG cryptography authorised for use within HMG can be considered to constitute "strong" encryption in export control terms, and will thus generally require an export licence in addition to CESG release procedures. BG cryptography based on CESG algorithms will attract similar constraints, but BG cryptography based on PD algorithms may well have a more flexible export posture, which is a major reason for the defence preference for unencumbered PD solutions at the BG level. The Defence ComSec Operating Authority should therefore be consulted before making any plans to move cryptographic systems from the UK or permanent overseas locations, having first reviewed the relevant BID or DIAN.

Installation of Cryptographic Equipment

2336. Installation of cryptographic equipment is only to be carried out by appropriately trained and cleared personnel.

2337. High Grade cryptographic equipment is normally CONFIDENTIAL but assumes the same level of protective marking as the cryptographic keymaterial when operational. Physical security to be provided is therefore dependent on the protective marking level of the operational machine; this may be achieved by installing the equipment in an appropriate security container as identified in the "Catalogue of Security Furniture". Where it is impractical to install within a container, e.g. because of the volume of equipment, rooms in which the cryptographic equipment is installed are to be of Secure Room Type A or B standard.

2338. Enhanced Grade cryptographic equipment where approved to process CONFIDENTIAL should be installed to the to the standards as laid down at Annex B. In all other case it is essential that good engineering practices, as laid down in JSP480, are observed.

2339. Baseline Grade cryptographic equipment is UNCLASSIFIED when it does not contain a cryptographic key. When filled with a cryptographic key either electronically or physically it must be protected in accordance with the protective marking of the key when operating attended. At cease work such devices must be switched off. When unfilled baseline grade devices must be protected so as to prevent theft, tampering or unauthorised modification.

Secure Containers

2340. Where cryptographic equipment is installed in a secure container, the container is to be firmly fixed to the fabric of the structure.

2341. Secure containers are not to be drilled or cut for access except through the panels provided for this purpose. The drilling of holes in any other part of a container renders it insecure and no longer approved for secure storage. (**JSP 440 Volume 1** refers).

Installation Standards

2342. Cryptographic equipment and associated terminal equipment is to be installed in accordance with TEMPEST regulations as detailed at **Chapter 21**.

Maintenance

2343. Maintenance of cryptographic equipment is only to be carried out by, or under the supervision of formally trained and cleared personnel.

Control by IDA/CIDA

2344. Installation Design Authorities (IDA) are to ensure that the design of any communications system to process protectively marked information is to meet the physical and COMSEC requirements of this document. A Co-ordinating Installation Design Authority(CIDA) is appointed for each MOD building or establishment, who is responsible for ensuring there is no conflict between individual systems processing protectively marked information. IDAs are responsible for advising and where necessary seeking approval from the appropriate CIDA before work is undertaken to provide secure communications installations.

2345. After installation, no changes are to be made to the configuration of a secure system without prior approval of the CIDA.

Cryptographic Spaces

2346. Where on-line cryptographic equipment and/or cryptographic material are not stored in lockable security containers, the areas containg these items are to be designated as cryptographic spaces, and access is to be restricted to personnel authorised by the CO/HOE. A list of authorised personnel is to be maintained, and visitors to cryptographic spaces are required to sign a register and give their reason for visiting. When they are in use, to ensure that they are not to be overlooked by unauthorised personnel, unmanned cryptographic spaces are to be secured by an approved security lock (see **JSP 440 Volume 1 Chapter 5 Section 1 Annex E**). Portable material such as keys, tapes and fill devices are to be locked away.

Compliance Checking

2347. The Defence ComSec Operating Authority is responsible for the enforcement of the policy laid down in this Chapter, specialist ComSec regulations relevant to the installation, and the BID(s) and DIAN(s) relevant to the cryptosystem, in accordance with **Chapter 12**.

2348. Additionally, where Baseline Grade (BG) cryptography is being used to provide desktop to desktop encryption between end user computer systems, the Accreditor may require that encryption keys be lodged at any MOD controlled Secure Managed Interface (SMI), as defined at **Chapter 15**, that is transitted to facilitate checks for Malicious Software **(Chapter 7)** and Transmission Violations **(Chapter 11)**.

Incident Handling

2349. The main threat to any cryptographic system is the possibility of the physical compromise of its keying material. The strictest possible control must be exercised over cryptographic material from the time of its production to its destruction.

2350. The loss of a cryptographic equipment, cipher, code, or any protectively marked associated document or the loss of any document which may prejudice the use of a cryptographic system constitutes compromise of the system.

2351. Any instance of physical violation, compromise or loss affecting cryptosystems must be handled as a matter of urgency by the Crypto Custodian(s) for HG or EG installations, and by either the relevant unit security officer (or a Crypto Custodian where one exists) for BG systems. A report must be raised to both the Defence ComSec Operating Authority and the Joint Security Co-ordination Centre (JSyCC) in accordance with **Chapter 11**.

Authentication by Cryptography

2352. Where Cryptographic Authentication is required, formally approved Digital Signature mechanisms should be used, details of which can be obtained from InfoSy(Tech). It should be noted that where cryptography is being used for Encryption / Decryption purposes to maintain Confidentiality, this cannot be assumed to automatically provide Cryptographic Authentication.

Integrity By Cryptography

2353. Where Cryptographic Integrity Checks are required, formally Cryptographic Integrity mechanisms (e.g. Cryptographic Checksums and Message Digests) should be used, details of which can be obtained from InfoSy(Tech) It should be noted that where cryptography is being used for Encryption / Decryption purposes to maintain Confidentiality, this cannot be assumed to automatically provide Cryptographic Integrity.

Interoperable Cryptography

2354. Most cryptographic systems in official defence use at present are those designed and built for UK government purposes, and their interoperability options, where applicable, are based on this model. A limited number of online cryptographic equipments of either UK or Allied origin can be configured to allow their interoperation with external entities, typically defence Allies, and it is important that any such interoperability requirement is identified to the Defence ComSec Operating Authority as early as possible in the procurement cycle.

2355. There is a growing requirement for use of BG PD cryptography to allow protected information exchange with wider range of external partners, who would not have been eligible for the release of cryptographic systems based upon CESG algorithms.

2356. Most early implementations of such technologies (e.g. *PGP for HMG*) rely on asynchronous communications techniques, and their interoperation can therefore be configured retrospectively if so required without a consequential risk of data loss.

2357. There is a growing requirement to extend such techniques to online cryptography, for example to permit the implementation of a Client-Server Virtual Private Network (CSVPN) as defined in **Chapter 22**, and such implementations should wherever possible be based upon Public Domain standards to obviate the risks of MOD becoming locked into any proprietary solution. The two major standards in this area are the *Internet Engineering Task Force* (IETF) *Internet Protocol Security* (IPSec), and *Transport Level Security* (TLS), and the standards underpinning their use for defence are contained at Annexes C and D respectively. The handling instructions for any product implementation of these standards will be found in the related DIAN.

.

ANNEX A TO

CHAPTER 23

CARRIAGE AND USE OF ENCRYPTION PROTECTED SYSTEMS ABROAD

Introduction

1. The aim of this Annex is to detail the current policy on the carriage and use of encryption protected portable IT equipment abroad. It is emphasised that these regulations do not affect any provisions already made for the use of such systems by a military forces deployed for operations or exercises, or for use by personnel on UK military bases outside the UK. This Annex is intended for those personnel who may be attending overseas meetings, courses and similar events in an official capacity and whose duties may require them to carry such encrypted systems. The importance of protecting portable systems containing protectively marked information cannot be overstated. It is emphasised that the key consideration in the overseas movement of such systems must be the maintenance of their security in accordance with JSP 440.

2. This Annex does not affect the restrictions and regulations for the movement of any other form of cryptomaterial or equipment.

Removal of Export Controls for Personal Systems

3. During the last year export regulations covering the import and export of cryptographic equipment and algorithms have been relaxed. This has come about as a result of an international agreement signed at Wassenaar in December 1998 and now formally incorporated into many nations' regulations and legislation. For instance, portable computer systems employing encryption products, and carried for personal use, should no longer be subject to export control in signatory nations. Examples of such products are Kilgetty, Secrets for HMG and Safedial modems. There is no longer any requirement to carry an Open General Export Licence for the movement of such systems overseas.

Open General Export Licence - Consumer Cryptographic Goods

4. The Department for Trade and Industry has updated its Open General Export Licence (OGEL) covering encryption protected systems and similar devices. The OGEL now covers the import and export of consumer cryptographic goods which are *not* being carried for personal use. There are no export controls on personal systems.

However, at Schedule 2 of the OGEL there remains a list of specifically excluded export destinations.

Specific Restrictions on Government Approved Encryption Products

5. MOD imposes specific restrictions on the movement of government approved encryption products for personal use. All products remain excluded from export to the list of destinations contained in Schedule 2 of the OGEL. Shown below are the restrictions on the movement of the following affected products:

a. KILGETTY

b. SAFEDIAL

c. Secrets for HMG

Schedule of Permitted and Excluded Destinations for Government Encryption Products

All Products

Excluded - (Schedule 2 of OGEL) Afghanistan, Angola, Armenia, Azerbaijan, Bosnia and Herzegovina, Burma (Myanmar), Burundi, Croatia, Democratic Republic of the Congo, Ethiopia, Eritrea, Iran, Iraq, Liberia, Libya, Nigeria, North Korea, Peoples Republic of China (excluding Hong Kong SAR), Rwanda, Sierra Leone, Somalia, Sudan, Tanzania, Uganda and Yugoslavia (Federal Republic of).

Additional Restrictions

Kilgetty
Permitted - NATO, EU, Australia, New Zealand, Sweden

Excluded - Eire (for KILGETTY PLUS), Rest of the World

Safedial
Permitted - World wide

Secrets for HMG
Permitted - NATO, EU, Australia, New Zealand

Excluded - Rest of the World

Prior to Travel

6. Notwithstanding the MOD list of approved destinations, personnel travelling overseas with encryption protected systems remain responsible for ensuring that they have the appropriate clearances for using such equipment in their destination country. This provision particularly applies when travelling to foreign military establishments, regardless of country, which may have additional regulations concerning the use of such equipment within them. The overseas point of contact or sponsor for a visit should be the focus for such enquiries.

Precautions during Travel

7. Security staff at airports or customs officials sometimes ask to see personal electronic equipment powered-up to establish that it has not been adapted for smuggling or use as an explosive device etc. To deal with such situations, travellers with systems employing encryption protection may wish to ensure that their computer contains some non-sensitive material that they can display if legitimately required to do so.

Points of Contact

8. Further advice regarding these instructions can be obtained from: InfoSy(Tech)ComSec (Tel: (9)621x80124)

This page intentionally left blank.

ANNEX B TO

CHAPTER 23

INSTALLATION REQUIREMENTS FOR ENHANCED GRADE CRYPTOGRAPHIC EQUIPEMENTS

Introduction

1. The aim of this Annex is to provide guidance as to both the physical and radiation security (RadSec) installation standards to be applied when installing Enhanced Grade (EG) cryptographic equipments.

Physical Security

2. The overall physical security requirement for the equipment will be governed by the maximum protective marking of material to be protected by the cryptographic equipment in question, in accordance with **Volume 1**. In addition, due to the valuable and sensitive nature of these equipments :

a. Any container used to protect the equipments should be secured to rigid part of the building structure ;

b. For RESTRICTED equipments intended to be left operating unattended, the baseline requirement for any locked room used to protect them will be the Secure Enhanced Room standard as laid down at **Chapter 5 Annex A.**

RadSec

3. The installation requirements will be determined by the highest protective marking of material to be protected by the cryptographic equipment in question:

a. Where CONFIDENTIAL material is to be protected, the equipments must be installed in accordance with both AMG-719 and JSP480 ;

b. Where RESTRICTED material is to be protected, the equipments must be installed in accordance with JSP480, with the additional stipulation that all RED elements of the equipments are to be separate by at least 500mm from any BLACK equipment.

This page intentionally left blank.

ANNEX C TO

CHAPTER 23

USE OF INTERNET PROTOCOL SECURITY (IPSEC)

Introduction

1. The aim of this Annex is to document the MOD requirements for any Baseline Grade (BG) implementation of the *Internet Engineering Task Force* (IETF) *Internet Protocol Security* (IPSec) standard, as outlined in *RFC2401*.

2. As the IPSec standard offers a number of potentially incompatible options, a generic MOD profile has been generated against which any IPSec implementations offered for CAPS BG approval will be endorsed, to obviate the risks of MOD becoming locked into any proprietary solution.

Requirement

3. There is a growing requirement for use of BG Public Domain (PD) cryptography to allow protected information exchange with wide range of external partners, who would not have been eligible for the release of cryptographic systems based upon CESG algorithms.

4. A particular requirement is to provide a means of online cryptography based on such an approach, both to facilitate Client-Server Virtual Private Networks (CSVPN) to permit cost-effective Secure Remote Access (SRA) solutions to be built, and also for Gateway-Gateway VPNs.

Profile

5. Any implementation of IPSec for MOD must :

   a. Provide *Authentication Header* (AH) functionality (*RFC2402*), which must support the *Secure Hash Algorithm* HMAC variant (SHA-HMAC) which provides an additional level of hashing as its authentication algorithm (*RFC2404* and *FIPS-180*) ;

   b. Provide *Encapsulating Security Payload* (ESP) functionality (*RFC2406*), with the encryption to be carried out using a Public Domain algorithm accepted for HMG BG use, the *de facto* standard being 3DES. This must be capable of being configured to support Tunnel-mode for Gateway-

Gateway VPN and Transport-mode for CSVPN;

c. Provide *Internet Key Exchange* (IKE) as laid down at *RFC2409* for negotiation of both user-orientated security associations (CSVPN) and/or host-orientated security associations (Gateway-Gateway VPN) ;

d. Provide *Internet Security Association and Key Management Protocol* (ISAKMP) as laid down in *RFC2408* to allow the optional anti-replay security service to be configured if required;

e. Be able to be generically configured, either using a custom distribution or preferably a custom configuration utility, to ensure that both the mandatory options are enabled by default, and that a conscious user action is required to deactivate such settings ;

f. Be approved for Government use as a Baseline Grade (BG) cryptographic product.

Dissemination

6. This Annex is an UNCLASSIFIED document that may be released to interested vendors, provided that such a release is made under the clear understanding that the contents are for Official Use Only, and may not be further released to 3rd parties without consent of the originator in MOD.

ANNEX D TO

CHAPTER 23

USE OF TRANSPORT LAYER SECURITY (TLS)

Introduction

1. The aim of this Annex is to document the MOD requirements for implementation of *Transport Layer Security* (TLS) standard, as outlined in *RFC2246*, in cases where Baseline Grade (BG) would otherwise be required.

2. This requirement is based upon CESG Infosec Manual T, as interpreted for the military environment. This document refer only to publicly available implementations of TLS and the products that use them. This pragmatic approach to this particular class of products **does not imply similar concessions for any other cryptographic products**. The UK Government's continued position is to evaluate as thoroughly as possible cryptographic mechanisms used to secure protectively marked data. In particular, inclusion in this document of a cryptographic algorithm, method or protocol does not imply CESG recommendation unless explicitly stated.

3. TLS can only be one component in securing a distributed system: the protocol does not protect the integrity or the confidentiality of any data stored on servers, or being processed within a client domain. It provides no protection against vulnerabilities present in the end systems or in the management of those systems. Other measures designed to assure overall system security may in some circumstances reduce or eliminate the requirement for TLS. It should also be noted that the advertised presence of TLS might mislead users into believing that better system security is present than in fact exists.

Background

4. The Transport Layer Security protocol has been devised by the Internet Engineering Task Force (IETF) as a non-proprietary development of the popular Secure Sockets Layer (SSL) protocol developed by *Netscape Communications Corporation*. For many purposes, TLS can be thought of as equivalent to SSL v3.1. TLS v1.0 was released in 1998.

5. TLS provides transport layer communications security for client / server based internet applications. Its primary use, so far, has been to provide a secure channel between world-wide web browsers and the web servers with which they wish to communicate. However, TCP port numbers are also defined for TLS for use with

SMTP (Simple Mail Transfer Protocol), NNTP (Network News Transfer Protocol), LDAP (Lightweight Directory Access Protocol) and POP3 (Post Office Protocol).

6. A complete list of the ports defined for TLS/SSL can be found at http://www.iana.org.

7. The official goals of TLS are "cryptographic security, interoperability, extensibility, and relative efficiency". These are very similar to the goals of SSL. The main changes in TLS v1.0 (from SSL v3.0) are minor security improvements, clearer and more precise specification, and a broader base for future protocols.

8. TLS enables client and server to secure a TCP connection by encrypting all traffic between client and server. The protocol does not provide confidentiality or integrity for data stored on the server, or when it is processed within the client domain.

9. The main benefits of TLS can be summarised as follows :

a. It is extensible and adaptive. It provides a means for two parties to negotiate which cryptographic protocols they will use to communicate ;

b. By separating functions, TLS allows different algorithms and different keys to be used for encryption, authentication, and data integrity. This is advantageous where national or local legislation places limitations on the lengths of certain types of cryptographic keys ;

c. In addition, TLS allows sessions which are not encrypted but which are authenticated and protected against tampering. This is useful in countries where encryption is forbidden by law, but data integrity is still desired ;

d. It is reasonably efficient. Because of the time-consuming nature of public key encryption / decryption, TLS allows session security data to be preserved between connections. This allows secure communications to begin immediately, without the need for extraneous public key operations.

10. TLS / SSL is the only encryption protocol that is present by default in the majority of desktop environments.

11. In summary, TLS is a communications security protocol and provides no protection against vulnerabilities already present in either communicating system. It protects the traffic against observation whilst in transit through the network between the TCP connection end points and authenticates those end points to one another.

Limitations

12. TLS only provides protection only between TCP end points and other

appropriate Infosec measures must be in place to provide protection outside of those end points.

Configuration

13. TLS is not a single product, but a protocol that is implemented, to varying standards and degrees of correctness, in several commercial products. Given that most problems in a given system are due to the implementation and that it will not be feasible to evaluate commercial implementations, CESG have taken a pragmatic view as to the configuration offering the best security for protectively marked data.

14. The RFC for the TLS protocol is constantly under review and the number of available ciphersuites is expanding. In particular, it is likely that the TLS standard will be updated in the near future to include one or more ciphersuites specifying the recently selected AES algorithm. It is therefore likely that situations will arise in the near future that are not covered by this document. Users who believe that such a situation applies to their project should contact InfoSy(Tech) for the latest recommendations.

15. Provided the requirement for encryption is no more than HMG Baseline Grade (BG), the way in which TLS can be used to provide confidentiality and authentication services is in the following configuration:

a. Only ciphersuites containing CESG-approved cryptographic elements may be used to secure protectively marked data. In the current TLS RFC, this equates to ciphersuites using:

i. Triple-DES as the data encryption algorithm;

ii. SHA-1 as the data integrity algorithm;

iii. DSA/DSS or RSA as the signature algorithm;

iv. Either RSA or Ephemeral Diffie-Hellman as the key exchange algorithm;

b. For key exchange algorithms, the composite modulus size must be 1024 bits.

c. For signature algorithms, the modulus must be 1024 bits with a 160 bit parameter;

d. Servers and clients must be configured to allow selection only of ciphersuites comprising recommended algorithms;

e. Only TLS products configured to authenticate always both the client and the server are to be used to secure protectively marked data;

f. Operating procedures should mandate a user to check manually the certificate as connection is initiated and before any protectively marked data passes over the connection;

g. Servers are to be configured to perform a check of the certificate as connection is initiated, and before any protectively marked data passes over the connection;

h. Identity certificates are not to be used as the sole method of authentication and identification; complementary Infosec measures must also be employed. The Accreditor should contact InfoSy(Tech) as early as possible in the system design cycle to validate these complementary measures;

i. Security Policy Documentation should mandate a maximum duration for the validity of retained session security data. This is likely to be project dependent, and system security managers should contact InfoSy(Tech) through their Accreditor before setting a value. In no case should session security data remain valid for more than 24 hours, after which a new key exchange process must be initiated;

j. To ensure that session security data is not compromised, a browser's cache must be explicitly flushed at the end of a TLS session;

k. It is reiterated that TLS provides protection only between TCP end points and other appropriate Infosec measures must be in place to provide protection outside of those end points.

Dissemination

16. This Annex is an UNCLASSIFIED document that may be released to interested vendors, provided that such a release is made under the clear understanding that the contents are for Official Use Only, and may not be further released to 3rd parties without consent of the originator in MOD.

MESSAGING SECURITY

This page intentionally left blank.

CHAPTER 24

MESSAGING SECURITY

Part 1: Interorganisational Messaging Security

Introduction

2401. An interorganisational ("formal") message is an Official message subject to formal release and commitment, that is legally binding under Engliish Law and Military Law, and is accountable. A Message Transfer Service (MTS) takes full responsibility for a formal message from its point of submission the point at which the recipient(s) accept staff procedural responsibility.

2402. **Description of the Service**. Formal signal messages are carried over the worldwide Defence Communications Network (DCN) which extends through gateways to diplomatic, NATO, allied and old Commonwealth nations. The formal message service is provided specifically to support the rapid transmission of operational command, control, logistic and administrative orders and reports, etc. required to meet the needs of Defence and the Diplomatic Service.

2403. Formal signal messages are sent under the authority of the unit or organisation and are authorised by a releasing officer - they are inter-organisational rather than interpersonal. Unlike other electronic means, formal messaging offers unique standards of service which support delivery within set time limits according to precedence and guarantee integrity and confidentiality according to protective marking, caveat, descriptor and any special handling instructions. These standards are defined in the UK supplement to Allied Communications Publication (ACP) 127 and associated ACPs.

2404. The use of electronic mail services, such as the ITU-T X.400 standard, for Interorganisational Messaging is not widely support at present, and these regulations therefore are limited to the Signal systems. Some generic guidance on electronic mail is given under Interpersonal Messaging Security later in this chapter.

2405. **Message Writing and Handling**. Instructions for the staff in writing and handling formal signal messages are contained in JSP 101 and single-Service publications. Messages are delivered and distributed via Communication Centres (COMMCEN). The delivery and distribution service may be manual, automated or semi-automated. Messages are submitted to COMMCEN either in paper form - F Sigs 266 and 266A (text continuation sheet), or electronically through an approved formal message application. Other objects (such as disk) or forms may be used provided they

meet the subject field requirements described in JSP 101 and are authorised by the OIC COMMCEN. In most large HQ, delivery and distribution is achieved through a Receipt and Delivery Centre (RDC) or a Registry.

2406. **Protective Markings, Caveats and Special Handling Instructions**. The vast majority of the DCN is approved for the transmission of protective markings up to and including SECRET. TOP SECRET messages and messages requiring the use of a caveat and/or a special handling instruction, are to be addressed to the Special Handling Cell in the COMMCEN. Details of how these messages are handled and delivered are contained in ACP 122 UK Supp-l(A) - TOP SECRET and Special Handling Messages.

2407. **Special Handling (SPH)**. TOP SECRET formal messages and those given a caveat and/or a special handling instruction are normally processed separately from non-SPH messages, in call cases by suitably vetted and indoctrinated staff. The channels used for such traffic are specially approved, and will support either greater authentication at each end or off-line encryption. STRAP and other Special Compartmented traffic is carried over entirely separate channels which are not described here. Most, but not all, major COMMCENs have the resources to process special handling messages. Staff should check details of the provision of special handling services with the local COMMCEN or CIS staff.

Protective Markings

2408. **Categories**. Messages are given a protective marking appropriate to the contents and circumstances in which the message is sent as either: 'TOP SECRET', 'SECRET', 'CONFIDENTIAL' or 'RESTRICTED'. Messages relating to certain subjects must always be given a protective marking; details at Annex A (reproduced from Annex D, Chapter 16 of JSP 101).

2409. **Message Form**. The protective marking is entered in the box or field provided and on every page of the message. If the message does not warrant a protective marking the word 'UNCLAS' is to be entered to indicate that security considerations have not been overlooked. Messages marked with a protective marking are handled in the same way as other protectively marked documents. COMMCEN are not permitted to accept messages which are not marked with a protective marking, or with 'UNCLAS' or 'CLEAR' (see paragraph 2410).

2410. **CLEAR Procedure**. In a tactical situation in which secure communications are not available and where time prohibits encoding and decoding, messages up to and including SECRET may be sent in CLEAR. The commander or his deputy must authorize each message sent in this way. The word 'CLEAR' is to be transmitted at the start of text indicating that the message contains classified information and has been authorized to be sent in clear. Original copies marked 'CLEAR' are to be handled as 'CONFIDENTIAL' material. The received version is to be marked with 'RECEIVED IN CLEAR TREAT AS CONFIDENTIAL'. Messages so marked are not to be readdressed. Where this is required, a new message is to be originated and handled as the situation demands.

2411. **Prefixes**. Current DCN gateways into other networks only support the IDO approved prefixes 'WEU' and 'NATO'. The use of any other prefix will cause the message switch or gateway to reject the message. Staff should also note that the words 'Classification', 'Classified' and 'Unclassified' remain valid international terms. (Only the UK has changed to calling classifications protective markings.)

2412. **Release Instructions**. Because most formal messaging networks do not recognise the prefix 'UK', the DCN cannot routinely support the instructions contained in JSP 440, Vol 1, Part 2, Chapter 11, Para 1164 to insert the prefix 'UK' before protective markings on formal messages to be passed to other countries. Instead, the drafter must apply the appropriate protective marking and insert the term 'UK CLASSIFIED RELEASED IN CONFIDENCE TO xxxxx' as the first words of message text. In other circumstances, CIS staff should obtain agreement on the use of suitable release instructions prior to an operation or exercise. Five Power Defence Arrangements (FPDA) exercises might use 'UK CLASSIFIED RELEASABLE TO FPDA'. Similarly, the NATO CIS authority might employ the textual instruction 'NATO CLASSIFIED RELEASABLE TO PFP' in NATO exercises or operations with PfP nations. UK protective markings in messages to addressees served by non-UK communications networks and the use of the special handling instruction 'UK COMMS ONLY' are covered in Annex B Chapter 16, Volume 1 Part 2 of JSP 440.

Descriptors

2413. Descriptors are used by UK Defence to indicate the sensitivity of material and the need to limit access. (They are not recognised by the international community.) Where a descriptor or descriptors are required (no more than two should be applied in the same message) they are written as the first words of the text followed immediately by a full stop. They are also entered at the top and bottom of the message form in the box marked 'Descriptor/Special Handling Caveat'. Example (start of text):

'MEDICAL. AIDS VIRUS UPDATE....' NO PLAY

No Play

2414. During exercises, the need to differentiate between exercise play and real activity, eg a real emergency of some kind, is accommodated through the use of the proword 'NO PLAY'. This is inserted as the first and last words of text, and in the Message Instructions box. 'NO PLAY' messages are subject to the same threat from intercept as all other message traffic; they must bear an appropriate protective marking. If insecure communications are used, the exploitable text of formal and informal signal messages must be encoded unless the time delay involved is likely to endanger human life. The international proword 'NODUF' (No Direction Finding) may be used by allied formations, but is not used in UK joint message procedures.

Releasing Officer

2415. Formal signal messages are unique in requiring the authority of a releasing officer who authorizes a message for and on behalf of the organisation which he or she represents. (The responsibilities of the releasing officer are described fully in JSP 101.) For convenience, the grades of officers required to release messages of each protective marking are given here.

a. **TOP SECRET**. An Officer not lower in rank than Commander RN, Lt Colonel, Wing Commander, Civil Service Pay Band C1, or by a Resident Clerk or a Private Secretary to a member of a Council or Board.

b. **SECRET**. An Officer, not lower in rank than Lieutenant Commander, Major, Squadron Leader, Civil Service Pay Band C2, or the equivalent.

c. **CONFIDENTIAL**. An Officer not lower in rank than Lieutenant RN, Captain, Flight Lieutenant, Civil Service Pay Band D or the equivalent.

d. **RESTRICTED**. Any Service Officer, SNCO or a Civil Service Pay Band E1 (or equivalent) or above.

2416. Requirements for exceptions to the above should be referred to both the Principal Security Advisor (PSyA) responsible for the unit or formation involved, and to DCSA Messaging at Corsham.

References

2417. **Unique Reference**. The combination of Date Time Group and Subject Indicator Code (SIC) is used as the originator's unique reference in formal signal messages, eg 'YOUR BDZ 121315Z JAN 98' and 'MODUK NAVY LGN 151624Z FEB 98'.

2418. Messages which refer to the text of messages or documents bearing a protective marking of CONFIDENTIAL or above should normally be given a protective marking of RESTRICTED or higher.

2419. A message referring to a document or message graded RESTRICTED may be sent as Not Protectively Marked (UNCLAS) provided only innocuous reference has been made to its contents.

Messages to Countries Presenting Special Security Risks (CPSSR)

2420. It must be assumed that all communications such as telegraph, telex and teleprinter to and from United Kingdom posts in CPSSR are subject to monitoring and analysis. In order to guard against the immediate exploitation of UNCLASSIFIED

information by intelligence services in CPSSR, the following procedures should be observed:

a. Signal messages to posts in CPSSR containing information which would normally be treated as UNCLASSIFIED, but which it is desirable to deny to CPSSR, should be protectively marked at least RESTRICTED and sent by protected means through Foreign and Commonwealth Office (FCO) channels. This applies particularly to signal messages about staff matters, including movements, pay, allowances, etc, of named individuals.

b. UNCLASSIFIED messages may be sent *en clair* to posts in CPSSR when the originator is satisfied than an interceptor could not deduce from the text anything about the functions or circumstances of staff stationed in, or visiting the post of chancery, military attache, commercial secretary, etc, that is not already public knowledge or available to the country concerned, eg informing a post that a visa has just been granted by a CPSSR to a named individual. Similarly, it may be possible to send a signal *en clair* by using such phrases as, person named in your letter etc;

c. The responsibility for deciding whether or not such messages to posts in CPSSR should be dispatched *en clair* or by protected means rests with the Releasing Officer. In cases of doubt, signal messages should be marked at least RESTRICTED and sent by protected means.

Dispensation for Individual Signal Accounting

2421. During Operations or exercises, the intensity of signal traffic protectively marked CONFIDENTIAL (CAVEAT) and SECRET may rise sufficiently that manual accounting for paper copies, over and above that provided by messaging systems, for these signals becomes impracticable. Under these circumstances, and when CO/HOEs have satisfied themselves that such levels have been reached, they may issue a written authorisation to relax the individual accounting rules for operation/exercise related CONFIDENTIAL (CAVEAT) and SECRET traffic. It is stressed that waivers are to be restricted to these specific signals, and non operation/exercise material is to be subject to normal rules. TOP SECRET signals are always to be accounted for individually. When such dispensations are in force, the Authorising Officer is to ensure that:

a. The number of copies of signals is kept to an absolute minimum. Signals are to be retained in an operational log maintained in the COMMCEN and checked at frequent intervals by a responsible person.

b. The rules for disposal of the material are strictly applied.

c. Any signal distributed to areas other than the COMMCEN must be subject to normal manual accounting rules (i.e. entered into the appropriate MOD F102.)

d. The relaxation is to apply for no longer than is strictly necessary, and the period is to be recorded in the original authorisation which is to be available to inspecting staffs as required. Cancellation of the relaxation is to be automatic on expiry of the quoted date. Any extension to the date must be authorised in writing following the above procedure.

2422. It is emphasised that relaxations are not to be applied simply because an exercise/ operation has begun, but must be governed by a genuine impracticability owing to traffic levels. Proper accounting procedures are to be resumed as soon as levels permit even though an exercise/operation may still be in progress. The Authorising Officer is to review the requirement for the relaxation at frequent (not exceeding weekly) intervals.

Use of Facsimile for Signal Messaging

2423. The policy on the use of facsimile for signal messaging is shown at Annex B.

Part 2 Interpersonal Message Security

Informal Messaging

2424. **Description of the Service**. Electronic mail ("e-mail") services, such as the ITU-T X.400 standard, or the *Internet Engineering Taks Force* (IETF) *Simple Message Transport Protocol* (SMTP) as laid down in *RFC822*, have been designed to provide informal "interpersonal" messaging services (IPMS).

Security within E-Mail Services

2425. The generic e-mail services provide little in the way of either security or message control facilities, although there a number of emergent standards that may provide security for e-mail :

a. **STANAG4406** - NATO X.400 messaging both Interpersonal and Interorganisational;

b. **ACP123** - Allied X.400 messaging, both Interpersonal and Interorganisational;

c. **CASM** - CESG Architecture for Secure Messaging.

2426. It should be noted that although there are several *de facto* commercial means of providing Confidentiality of e-mail by encryption, such as *PGP* and *S/MIME*, they are not approved for use with Protectively Marked information unless both a CESG Assisted Product Scheme (CAPS) approval and the associated Defence Information Assurance Notice (DIAN) has been issued.

2427. When selecting a interpersonal messaging service for an MOD organisation, other than client software (User Agents) to provide simple Internet mail reader / sender capabilities, it is recommended that Sector CIS authorities be consulted a to any future plans for standardisation, to avoid nugatory spend.

Disclaimers

2428. As e-mail is not a formally recognised form of interorganisational messaging, it is generally recommended that the following style of "disclaimer" is added below the signature block to highlight the lack of a formal Release Officer function when sending messages without an organization :

> <Name>
> <Post Title>
> Ministry of Defence
> mailto:<e-mail address>
> tel:<telno>
> fax:<telno>
> --
> The information contained in this e-mail and any subsequent correspondence is confidential and is intended solely for the recipient, for those other than the recipient any disclosure, copying, distribution, taken or omitted to be taken in reliance on such information is prohibited and may be unlawful.

2429. If, while linked to a public data network, the auto response is set so that the message transfer service (MTS) generates a receipt for in coming e-mail, the following text should be used:

> "The recipient acknowledges that the MOD is unable to exercise control over the content of information contained in transmissions made via the Internet. The MOD hereby excludes any warranty as to the quality or accuracy of any information contained in this message and any liability of any kind for the information contained in it, or for its transmission, reception, storage or use in any way whatsoever."

Mail Distribution Lists

2430. A convenience tool provided by manner Mail User Agents (MUA) is the ability to store Mail Distribution Lists, grouping together addresses. It is important to review such list regularly to ensure that persons no longer intended to receive email are not inadvertently distributed when an old mailing list is expanded for distribution.

Connection of Internet Mail Service

2431. Specific considerations apply when sending mail (limited to UNCLASSIFIED) to Internet addressees, as laid down at **Chapter 10**. In particular, if the mail has originated from a system processing Protectively Marked material, part of the release

sanction process must involve both the explicit authorisation by the user to send the item to the Internet, and the removal of any indication (e.g. the plain text work UNCLASSIFED in the header) that the message may have come from anything other than an UNCLASSIFED source.

ANNEX A TO

CHAPTER 24

MANDATORY PROTECTIVE MARKING OF SIGNAL MESSAGES

1. All messages containing information concerning matters listed in this Annex **must not**, subject to any exception stated in this Annex, be sent as UNCLAS messages, but must be given an appropriate protective marking.

2. **Movements of Ships and Units**.

a. In time of war and periods of tension.

b. In time of peace, movements which:

(1) Have strategic or political implications.

(2) Are more than 14 days ahead; nevertheless, the CinC, flag officer or senior officer concerned has discretion to advance or postpone the date of the downgrading provided that, in the former case, clearance, where required, has been obtained and local civil authorities have been informed.

(3) Are less than 14 days ahead but, in the case of Commonwealth or foreign countries, clearance is still awaited, or, in the case of courtesy visits to British non-naval ports, the local civil authorities have still to be informed.

c. Exercise and training programmes and details of ships and unite taking part in a particular exercise except when such information has been specifically declassified.

d. Sailing signals for HM ships and for Royal Fleet Auxiliaries (RFAs) operating with the fleet.

e. Daily position reports from units in c.

f. Weather reports which include ships' positions; nevertheless, when HM ships encounter extremely severe weather or detect indications of a tropical storm in the vicinity they should, operational requirements permitting, make an

unclassified non-routine report to the appropriate Commonwealth radio station and nearest weather centre.

3. **Intelligence**.

a. Matters affecting diplomatic relations.

b. Intelligence and counterintelligence matters.

c. Information concerning foreign countries.

d. Military information.

4. **Scientific**.

a. Problems under investigation by scientific research experimental establishments.

b. Results of trials sponsored by research establishments.

c. The location of future trials.

5. **Technical**.

a. Manufacturing processes, methods or production and technical details of warships, aircraft, weapons and equipment.

b. Existence of new weapons and equipment.

c. Reports on trials of new technical equipment.

6. **Communications**.

a. Codes, cyphers and other means of communication providing security.

b. Radio organization or references to frequencies.

c. Mail diversion messages and messages giving diversion instructions for drafts and stores.

d. Electronic warfare.

7. **Personnel**.

a. Movements of ships and other matters which might affect the morale of the fleet.

b. Reports on the morale of forces.

c. Strengths of operational units.

d. Outbreaks of epidemics.

8. **Logistics**. Logistics requirements and fuel state messages from frigates and above and replenishment at sea (RAS) RFAs are always to be protectively marked. Such messages from non HAS RFAs and ships below frigates are to be protectively marked on their merit.

This page intentionally left blank.

ANNEX B TO

CHAPTER 24

POLICY ON THE USE OF FACSIMILE FOR SIGNAL MESSAGES

General

1. Facsimile Systems are not part of the Defence Communications Network (DCN) and do not support the integrity and accounting functionality provided by ACP 127 networks. However, facsimile offers a perfectly legitimate means of clearing formal signal messages. Policy is provided here primarily to provide guidance for COMMCEN personnel and staff, to specify responsibilities and to define a minimum set of common procedures throughout Defence.

Acceptance and Delivery

2. Unless suitably equipped and approved by a unit's command HQ, COMMCENs are under no obligation to accept messages for clearance by facsimile. Where this is not the case, clearance is a staff branch responsibility. COMMCENs shall only accept messages for delivery to addressees which are expressed as valid Signal Message Addresses (SMA). (SMAs are listed in the ACP 117 series of publications and are held by COMMCENs. JSP 203 explains the composition of SMA.) This applies equally to Address Indicating Groups (AIGs), see below, and General Message Titles (GMT), used by the RAF, which are a collective form of SMA. (AIG details are contained in JSP 202.) COMMCENs may achieve onward delivery to addressees by facsimile where this method of transmission has been approved. COMMCENs are not responsible for the reproduction or distribution of additional copies of signal messages.

AIGs - Delivery by Facsimile

3. Sponsors of AIGs who wish to include an addressee for whom delivery can only be achieved by facsimile in an AIG, are required to contact their command HQ CIS branch for them to nominate a COMMCEN (equipped with facsimile) to be responsible for onward delivery to the addressee. Having obtained command HQ CIS branch authority in this way, sponsors shall inform CDCN and DCPB so that details may be entered into routing data bases and publications.

Facsimile Security

4. The security rules governing the use of facsimile equipment are shown at Chapter 18. Violations are also to be reported in accordance with the instructions contained in Chapter 4 to ACP 121 UK SUPP-1(A).

Precedence

5. All levels of precedence may be cleared by facsimile; but, unless a facsimile terminal is known to be manned, signal message precedence shall be limited to Routine. Formal signal messaging rules apply to delivery out of hours and to closed stations.

Receipts

6. It shall be possible to conduct a full audit trail for all signal messages transmitted by facsimile.

a. An automatic or manual log of all transactions shall be maintained.

b. The onus is on the sending station to ensure that a receipt is obtained for every message.

c. Automatic receipts shall suffice for Routine messages. A manual receipt is to be obtained for Priority and above this may take the form of a telephone call or a separate facsimile message. All receipts are to be recorded.

SECURITY IN WIDE AREA (BEARER) NETWORKS

This page intentionally left blank.

CHAPTER 25

SECURITY IN WIDE AREA (BEARER) NETWORKS

Introduction

2501. This Chapter deals with the security requirements for the carriage of official information across wide area (bearer) networks, where a wide area or bearer network is defined as one that crosses the perimeter of a MOD Global Security Environment (GSE).

2502. These requirements therefore predominantly relate to the commercially furnished public bearers, whether provided by landline (copper or fibre-optic) or radio link (broadcast or point-to-point), which form the majority of the MOD bearer network capabilities.

2503. Most MOD-provided wide area bearer network services are furnished by the Defence Communications Services Agency (DCSA), and the security requirements and restrictions on the use of their services are laid down in the Code of Connection (CoCo) for the affected service(s). Details of DCSA CoCos can be obtained from DCSA Infosec on Corsham military extension 3073.

2504. If other instances are encountered where MOD is to provide its own wide-area communications bearers, the same general principles should normally be applied unless agreement is obtained from either the TLB or Trading Fund Principal Security Advisor (PSyA) concerned, or the DSSO, with regard to designation of such bearers as Controlled, Protected or Approved Circuits in accordance with **Chapter 22**.

Principle

2505. The starting assumption for the use of any publicly provided, or encrypted MOD provided, wide area bearer circuit is that it should not be used to carry any unencrypted (RED) official information protectively marked RESTRICTED or above unless there is specific guidance given in this Chapter.

2506. In no cases should any such circuits be used for the unencrypted transmission of information of information protectively marked CONFIDENTIAL and above without the approval of either the PSyA concerned or the DSSO.

2507. Appropriate grades of encryption for protection of official information transitting a GSE boundary are laid down at **Chapter 23**.

Use Of Public Bearers

2508. For many years MOD operated under a dispensation permitting transmission of RESTRICTED without encryption on public networks within the UK, but under a Pan Governmental decision in 1991 this waiver was removed.

2509. A transition timetable was therefore promulgated, requiring all systems to be protected by 31 Mar 98. However, subsequent to that mandate, national communications security requirements have been relaxed, in line with the risk management philosophy endorsed following the Cabinet Office Review of Protective Security (RPS).

2510. The revised Threat Assessment for RESTRICTED has indicated that there is no longer a general requirement for encryption for Traffic Confidentiality purposes within the UK mainland, but due to different threat criteria, this excludes Northern Ireland, will still requires encryption of RESTRICTED information. This Policy does not cover use of public packet-switched data networks (e.g. “Internet”), and specific policy for this is contained both later in this Chapter, and at **Chapter 10**.

2511. Although these revised rules cover the Confidentiality of information in transit, end-systems using unprotected wide area bearers need to have a system/installation specific Security Risk Assessment carried out, to cover all three elements of Confidentiality, Integrity and Availability.

System Considerations

2512. The level of protection of the communications is considered as part of the system risk assessment, which is to be carried out in accordance with the National Minimum Standards, on which technical elements of the Accreditation plan will be based. The following sections consider generic issues for both dial-up and permanent circuits.

2513. In particular, Accreditors are concerned over the risk of a static password, irrespective of its strength, being carried *en clair* across a public network, as compromise of the password can subvert the Confidentiality, Integrity and Availability of the whole system, rather than the just the Confidentiality of the subset of data carried across a compromised link.

2514. In carrying out a risk assessment therefore, the option of providing encryption as an "anti-hacking" measure may be more cost effective, or indeed feasible (no automated One-Time-Password or Challenge-Response system at present has been either Approved by CESG as a ComSec device or Certified under ITSEC/CC), than the CompuSec alternative(s) to protect against all the Threats and Vulnerabilities identified above.

Bearer Security : Dial-Up Circuits

2515. Where RESTRICTED data is to be carried over Dial-Up circuits (PSTN or ISDN), encryption will not be required as a ComSec measure within the UK mainland, as although no telephone system, whether it be MOD, Government or Public Telephony Operator (PTO) provided, is fully secure, and calls are vulnerable to interception and overhearing, the following non-security factors do provide some element of protection :

a. **Dilution Effect**. It is technically difficult and expensive to identify and extract particular telephone calls when they are 'mixed-in' with the myriad of telephone calls that make up the rest of Telephone Networks at any one instant.

b. **Dispersion Effect.** The dynamic routing of calls over Telephone Networks further complicates the targeting of particular traffic since a call between two points, if repeated, is unlikely to be routed via the same channel on both occasions.

c. **Compression and Multiplexing.** Most communications media incorporate features enabling the maximum amount of data to be sent down a given channel. Compression and multiplexing techniques are often applied to communication channels to eliminate the otherwise redundant capacity taken up by the natural pauses in conversation, thereby achieving a higher capacity network. Though utilised for mainly commercial reasons, such features deter casual access to the information being passed and thus afford a further degree of inherent security.

2516. In all cases where "dial in" connections are to be provided to IT systems handling other than purely UNCLASSIFIED data, these should have "dial back" functionality of at least the following set of features, to reduce the residual risk from the insecure bearer connection to be dealt with by the attached IT system

a. The caller should be authenticated by the dial-in modem or port protection device by both an ID code and password as per Chapter 6 Annex A ;

(i) The password should be inherently "non-guessable", within the limitations on format imposed by the dial-back unit ;

(ii) ID codes should not be obviously linked to the number to be dialled, and should not start with a numeric ;

b. The dial-back unit must only generate the return dial-back number from its own tables:

(i) The unit database must be managed to preclude "roving"/"free dial", where either the supplied ID is called or a “pass through” occurs when no dial-back number is in the table ;

(ii) Additional data supplied by the caller or the PTO (e.g. calling line identifier (CLI) / caller display system (CDS) should not be relied upon as part of the generation ;

(iii) The dial-back number should not be a line which has call redirection services available to preclude unauthorised / unnotified mis-diversions ;

(c) Measures be provided to ensure that a new path through the public network is provided for the dialled-back call to preclude line seizure

(i) If the same PSTN circuit is to be used for both incoming and outgoing calls, the dial back unit must being capable of "force disconnecting" the incoming call. For normal, 2 wire, PSTN circuits this can be achieved by changing the line impedance appropriately for greater than the 30 seconds "debounce" window to ensure a full "call clear" by the exchange line card circuits ;

(ii) If separate PSTN circuits are used for both the incoming and returned calls, or for ISDN circuits where the out of band signalling manages the call, no additional measures will be required for this aspect.

2517. The details of the dial-back system should be included within the System or Network Security Policy, and its use must be reinforced by Security Operating Procedures (SyOPs).

2518. In cases where the dial-back modem is integrated with the system's Identification and Authentication mechanisms, then its functionality and assurance should be calculated in accordance with National Minimum Standards, including the systems considerations for passwords *en clair*, and included within the Security Policy Documentation (SPD) for agreement with the Accreditor.

2519. For ISDN2e dial-up circuits, care must be taken to ensure that the signalling (D) channel is not configured for user data, as this can provide and “always on” connection without any indication to the end user.

Bearer Security : Point-To-Point Circuits

2520. Where unencrypted RESTRICTED data is intended to be carried over Permanent, Point-to-Point Circuits, including Private Wire (PW), Leased Lines and Private Circuits, it will first require to be accepted as a Protected Circuit, as defined at

Chapter 22. The following criteria must be met for RED (unencrypted) Protected Circuits, and in any other case Baseline Grade (BG) encryption will be required :

a. The Protected Circuit must be wholly constrained within the UK mainland ;

b. Evidence must be provided that no radio path is used within the following segment(s) of a Protected Circuit in its standard configuration, and if circuits are diverted radio paths in emergency or for maintenance, immediate notice subsequent to the event will be given to the user organisation:

(i) As part of the first or final link of the transmission ;

(ii) Across, or with a backlobe that extends across, water navigable by

(iii) seagoing vessels, excluding internal waterways.

(iii) Anywhere within the Greater London area.

c. The connected terminating locations must afford appropriate physical and technical protection for RESTRICTED information, subject to the approval of the Accreditator(s).

Bearer Security: Private Networks

2521. The transmission of unencrypted data protectively marked RESTRICTED or above is not generally permitted over "always on" Private Networks (i.e. those that are not constituted from dedicated, permanent, point-to-point elements), which includes technologies such as the xDSL (Digital Subscriber Loop) family (of which Asymmetric DSL (ADSL) is the most commonly encountered), broadband cable, and the "D" channel services on ISDN installations. This applies to both those provided by Public Telephony Operators (PTO), and to those provided by Cable Companies.

2522. The following technologies have been granted specific approvals by the UK Infosec National Technical Authority, CESG :

a. **SMDS** The Switched Multi-Megabit Digital Service (SMDS) is permitted for the carriage of information protectively marked RESTRICTED and below within the UK mainland only provided that this is solely provided and managed by British Telecommunications plc (BT);

b. **X.25** Public packet switched networks built using the International Standards Organisation's (ISO) X.25 protocol, when configured to provide Permanent Virtual Circuits (PVC) that are solely constrained to the UK mainland and are solely provided and managed by British Telecommunications

plc (BT) may be used for the carriage of information protectively marked RESTRICTED and below.

2523. Where additional technologies are identified for which no specific statements are made in this Chapter, InfoSy(Tech) should be approached though the PSyA or DSSO as appropriate for guidance before any procurement action is initiated. Frame Relay and ATM technologies have already been so identified, and detailed guidance will follow in due course.

Documentation Requirement

2524. In all cases, the use, or lack of use, of encryption for RESTRICTED circuits transiting the secure boundary of the site(s) must be clearly identified in SPD along with the grounds for the decision within the context of this guidance.

2525. In cases where encryption is required under these rules, please contact the Defence ComSec Operating Authority at DCSA.

2526. It should be remembered that this is intended as generic guidance only, and, as with all installations, the Security staffs and Installation Design Authorities (IDAs) may need to vary the requirements to meet the particular scenario for each system.

Connection to The Internet or Other Public Data Networks

2527. Connection to public data networks such as INTERNET is becoming an essential requirement for many Defence applications, and this topic is covered in detail at **Chapter 10** for connection of standalone systems. Additionally, where connection to larger infrastructures is involved, **Chapter 15** should be consulted.

Virtual Private Networks

2528. Virtual Private Networks (VPN) provide a means to achieve what to the end user seems like their own provide connection over a shared infrastructure, provided either internally or externally to the user's organisation. Within MOD, 2 distinct type of VPNs are defined :

a. The **Service Provider Furnished VPN** (SPFVPN), where bearer infrastructure services provide logical and/or cryptographic segregation of tunnel(s) between Service Attachment Points (SAP). This is equivalent to Hop-to-Hop (link) encryption, and provides no protection of the RED link between the SAP and the end system, and the amount of trust that can be placed in the protection of the RED envelope "in flight" is limited by the degree of trust that can be placed in the Service Provider (SP).

b. **Client-Server VPN** (CSVPN), where cryptographic security mechanisms provide segregation of communications data between clients and

servers using a shared infrastructure. This is equivalent to end-to-end encryption, and provides cryptographic protection of the RED data throughout the BLACK flight to the degree of trust that can be placed in the cryptography, but does not normally provide any envelope protection.

2529. When selecting a VPN, the above constraints must be considered and reflected in the Security Policy Documentation (SPD) of the CIS(s) being implemented.

This page intentionally left blank.

RADIO FREQUENCY (RF) DEVICES

This page intentionally left blank.

CHAPTER 26

RADIO FREQUENCY (RF) DEVICES

Introduction

2601. The use of the Radio Frequency (RF) elements of the Electromagnetic Radiation (EMR) spectrum is very attractive as a carrier for communications, due to its range, speed, and high traffic capacity. RF is therefore used as a carrier for a number of modes of transmission, including telephone, telegraph, facsimile, speech, data and television.

2602. The major disadvantages of radio is that it is more susceptible to interception than all other means of transmission, with it being neither possible to conclusively prevent such interceptions, nor possible to detect the unauthorized interception and recording of transmissions. In an operational environment, it will often be the case that brief and irregular interceptions can be sufficient for both direction finding (DF) and some Traffic Flow Analysis (TFA).

2603. It can be assumed that an Attacker can intercept RF transmissions with Commercial Off The Shelf (COTS) equipments at the following ranges as a guide:

a. **Frequencies below 30MHz** The propagation modes at these frequencies make it difficult to make any sensible guess as to the maximum possible intercept range, and therefore all such transmissions should be assumed to be liable to regular if not continuous interception ;

b. **Surface transmissions above 30MHz** Although a number of extremely variable factors such as mode of propagation, type and height of antenna, weather conditions and sunspot activity make it impossible to give precise maximum possible intercept ranges. Indeed, it is not even possible due to varying topographical factors to give a generic statement as to what constitutes Line-of-Sight (LOS) for transmission, although if high ground is used for a transmitter this may be up to 50km. The following broad classification may therefore be used in assessing the risk of interception of broadcast transmissions :

Distance from Attacker (Threat Source)	Risk Level
Less than 50km	VERY HIGH
Between 50km and 180km	HIGH
Between 180km and 600km	MEDIUM
Between 600km and 2,000km	LOW
More than 2,000 km	VERY LOW

Where a scatter mode of propagation is employed, transmissions are particularly vulnerable as they can be intercepted for appreciable periods of time in unintended directions.

c. **Airborne transmissions above 30MHz** The area of HIGH risk will be dependant on the relative heights of the transmitting airborne platform and the interceptor. Assuming the interceptor is at sea level, the following maximum possible intercept ranges should be used as a guide :

Transmitter Altitude	Intercept Range
3,000m	225km
10,000m	375km
15,000m	500km

EMSEC / EMCON

2604. MOD is concerned with security of deliberate emissions, such as those from Radio, Radar and Telemetry systems. The technical security measures taken to prevent information being available to unauthorised personnel from electronic emanations of communications equipments is referred to as Emission Security (EMSEC), and it, along with the related topic of Emission Control (EMCON), which is used in an operational environment to counter Direction Finding (DF) is covered in Service communications and OpSec publications.

RADHAZ

2605. In addition to security concerns about the operation of RF devices on MOD sistes or platforms, or by MOD personnel, the issue of Radiation Hazard (RadHaz) should also be considered, which is covered in Service communications and OpSec publications.

Voice Procedure

2606. The use of incorrect procedure, lack of thought before speaking, and individual mannerisms on voice radio nets combine to create a major source of insecurity.

2607. It is essential that all those who use voice radio are well trained in correct voice procedure and thoroughly practised in its use. Although the availability of speech security equipments on voice nets is becoming more common, the requirement for knowledge of correct procedures and the need for a high degree of net discipline still remains.

2608. Detailed instructions on voice procedure are laid down in Service communications and OpSec publications.

Transmitters On Mod Sites

2609. Secure communications and IT installations are designed to take into account any RF transmitters in the immediate locality, and it is the responsibility of Commanding Officers (CO) or Heads of Establishment (HOE) to ensure that the Co-ordinating Installation Design Authority (CIDA) responsible for the site is made aware of any RF transmitters located on their site.

2610. Additionally, the CO/HOE should ensure their staff are aware of the need to be vigilant for RF transmitters being installed proximate to the site boundaries, and for the CIDA to be informed should such equipments be installed.

Private Radio Networks

2611. A variety of private radio networks are offered, generically referred to as Private Mobile Radio (PMR). This includes proprietary networks (e.g. Cognito) and the emergent Terrestrial Trunked Radio (Tetra) standard. Many of these can be used in a manner analogous to mobile phones, as laid down **Chapter 18 Annex E,** and additionally act as mobile radio data systems.

2612. At present not PMR or mobile radio data systems are approved for the transmission of any Protectively Marked information, and all terminal equipments are to be controlled in a manner analagous to mobile phones whilst on MOD sites, which will typically involve their being completely powered of to disable any "always on" components.

Portable Transmitters

2613. Secure communications and IT installations are designed to take into account any RF transmitters in the immediate locality. Whilst it is relatively simple to compensate for fixed transmitters, portable devices could compromise any unencrypted information being processed on IT equipments in the vicinity. It is therefore necessary to impose restrictions on the use of portable RF transmitters.

2614. Where portable radio transmitters are officially provided for security purposes, i.e. by members of Ministry of Defence Police ((MDP) or MOD Guard Service (MGS), these are normally prohibited from being used in buildings where information protectively marked at CONFIDENTIAL or above is electronically stored, processed or forwarded, or in any other area so designated by the CIDA, except in emergency situations. Certain specialist portable radio transmitters can be safely used in these environments, and advice should be sought from the CIDA if so required.

2615. Where a requirement is identified for the use of portable radio transmitters within the perimeter of an MOD site or establishment for reasons other than security, **provided this is not within areas where protectively marked information is electronically processed or is discussed**, the Commanding Officer or Head of

Establishment may approach the appropriate PSyA and the CIDA for approval. Special attention is to be paid to contractors using portable transmitters.

2616. All users of portable transmitters are to be briefed on their use and the dangers of using a transmitter in a radiation hazardous area such as in the vicinity of explosives.

2617. Issues specifically dealing with mobile (portable) and cordless telephones are dealt with in **Chapter 18**.

Wireless Networking

2618. The use if wireless networking technologies to carry Official information is governed by Controlled Circuit regulations, as laid down at **Chapter 22**.

2619. Additionally, care must be taken to ensure that no technologies based upon wireless technologies (e.g. "Bluetooth" or RF based Identification and Authentication (ID&A) mechanisms) are enabled on systems used to store, process, or Official information, unless specifically so sanctioned by the relevant Accreditor, and documented in Security Policy Documentation (SPD).

Amateur Radio And Citizens Band Radio

2620. Although it is not desirable to restrict unduly holders of amateur radio or citizens band radio transmitting licences in pursuit of their hobby, the nature of these activities requires that such people should be fully aware of the possible security dangers which could result through failure to observe the principles of security.

2621. The following rules are to be observed by all personnel operating amateur/citizen band radio transmitters:

a. An operator of an amateur/citizen band radio transmitter must report the fact to his Director/Head of Establishment via Branch or Establishment Security Officers ;

b. Citizen Band transmitters either when permanently fixed in a vehicle or carried by hand are in no circumstances to be operated within MOD Buildings or Establishments and their outstations or areas under their control ;

c. Amateur radio transmitters may only be operated from officially authorised and licensed premises on MOD property in Amateur Radio Clubs ;

d. An operator is not, during a radio transmission or in subsequent correspondence with radio contact, to make any reference to his or her establishments official activities or to any subject of MOD or Service interest such as composition of any force or unit, the nature of its work, its equipment, its role in operations or exercise or Service movements generally ;

e. An operator is not to give any indication in his acknowledgement of reception (QSL) cards, or in any entry in any publication, of his employment on work of a sensitive nature or having any access to protectively marked information ;

f. An operator is to notify his Director/Head of Establishment or Establishment Security Officer immediately any written, or oral communication including QSL cards expressing interest in service or political affairs, which he received as a result of a radio contact with an operator, especially one from any foreign country. Any comment or question of a similar nature arising during the course of a radio contact is also to be reported ;

g. Care should be taken in following up personal contacts made through radio clubs. These should be kept to normal social and amateur/citizens band radio channels. The Director/Head of Establishment or their security officers should be informed of any attempt to take advantage of such friendships.

2622. The operation of any unlicensed equipment is strictly forbidden.

2623. The Director/Head of Establishment is responsible for ensuring that all holders of amateur/citizen band radio transmitting licences are fully briefed on the possible security dangers, and that they understand the rules and the need for complying with them. The Director/Head of Establishment should notify the appropriate PSyA of any incidents reported under sub-paras f and g.

2624. The rules given in paragraph 2621 apply also to personnel interested in amateur radio who operate only receivers, but who also correspond by letter or QSL card with other amateur operators.

Mobile Satellite Services

2625. Mobile satellite services are offered by a number of companies, the most widely used being the International Maritime Satellite Organisation (INMARSAT) personal service, INMARSAT M. Thus is a portable satellite terminal housed in a briefcase, which allows the user to connect to the PSTN form anywhere in the world. Communications to and from such terminals are vulnerable to interception, and mobile satellite service terminals must not be used for protectively marked material without the use of an appropriate grade of approved encryption, as laid down at **Chapter 23.**

Radio Microphones

2626. All radio microphones and PA systems currently in production and use from Commercial Off The Shelf (COTS) sources use unencrypted RF links, and as such are not normally to be used for other than UNCLASSIFIED purposes.

2627. Should a requirement be identified for the use of such technologies for RESTRICTED material, approval may be sought on a case-by-case basis from both the PSyA and the CIDA, provided that :

a. The site is within the UK mainland ;

b. The equipment is to be installed and operated from within a solid structure such as a brick building ;

c. At least a 100m controlled zone exists between the structure and the perimeter of the MOD site.

INTRODUCTION TO ACOUSTIC SECURITY

This page intentionally left blank.

CHAPTER 27

INTRODUCTION TO ACOUSTIC SECURITY

Introduction

2701. An often overlooked aspect of security is the issue of protecting information when carried in an acoustic (sound) form. The aim of this Chapter is to state the regulations and practices that will be encountered within the working environs of the MOD and associated establishments.

Responsibilities

2702. Line Managers are responsible for ensuring that staff under their control are briefed in the aspects of Acoustic Security relevant in their work as laid down in this JSP.

Scope

2703. Acoustic security covers 2 majors areas of interest:

a. Security of conversations ;

b. Security of emissions.

2704. This Chapter covers the basic principles of Audio security, which are the means to protect the conversations of MOD personnel. More detailed advice is provided in later Chapters to cover the more specialist topics of Acoustic security:

a. Counter Eavesdropping ;

b. Structural Acoustic Protection ;

c. Acoustic Emission Security.

Threat

2705. The general threat against information carried in Acoustic form is covered in the ***Annual Threat Assessment*** which is issued by the MOD Departmental Security Officer's staff (DDefSy and the DSSO), and thereafter promulgated to the Principal

Security Advisors (PSyAs) in all TLBs and Trading Funds. COs/HOEs requiring specific threat guidance should initially contact their PSyA who will seek specialist advice from InfoSy(Tech).

2706. The main elements of the Audio security threat are:

a. The threat from deliberate attempts to overhear conversations posed by FIS (especially at locations overseas), sophisticated terrorist and subversive organisations and in particular from criminals, investigative journalists, private investigators and some members of the public. This depends very largely upon the attacker's ability to gain access to the site of the target conversation. As with most forms of security, there is always a significant risk of an "insider" attack, where someone with legitimate access is suborned.

b. The threat from conversations accidentally being overheard by those not party to the information. This can be a result of simple proximity (for example unguarded conversations in communal areas), or an indirect effect exacerbated by technical means (for example a nearby microphone in a telephone or public address system).

2707. The threat posed to an individual or area can increase under certain circumstances. This might be because of media interest, major financial events, evidence or suspicion of information loss through eavesdropping, or for other reasons.

2708. The threats associated with the protection of sensitive conversations within MOD facilities and platforms against deliberate attack are detailed in **Chapter 28** (for active eavesdropping), **Chapter 29** (Structural Acoustic Protection), and **Chapter 30** (Acoustic Emission Security) for non-audio emissions (e.g. Sonar).

Principles

2709. Good practice and common sense can provide most of the security required for the less sensitive conversations that routinely occur within the MOD, where the bulk of the information discussed will be at the UNCLASSIFIED or RESTRICTED levels. The protection of occasional discussions at higher Protective Marking levels, randomly distributed in time and space and diluted by the mass of other information is aided by a culture of ongoing good practice.

2710. All conversations are inherently vulnerable unless the potential attacker can be denied access to the vicinity of them. The vulnerability relates to the area in which the conversation is being held. An understanding of the basic principles will help determine the need for appropriate countermeasures.

2711. The single most important countermeasure is an awareness amongst staff of the security risk associated with overhearing. This will involve promoting security awareness amongst new and existing staff through security lectures (including

induction lectures) and other courses, and distribution of awareness material. It will be intended to warn staff not to discuss sensitive matters in public places or where they can be overheard by uncleared visitors, contractors etc.

2712. Additionally, staff must be aware of the need to actively reduce the risk of casual overhearing by closing doors (and windows if necessary) when holding sensitive discussions.

2713. Good building access controls will be the main deterrent to any potential eavesdropper. Good building design is important, and the incorporation of sensitive zones sited away from vulnerable points (i.e. adjacent to public areas or toilets, or on ground floor perimeters) is recommended. Staff should be well briefed on the need to prevent unauthorised access; the regime should be supported by suitable pass and access control systems. There should be control and supervision of visitors and staff with limited clearances (e.g. cleaners, maintenance staff etc).

Control Of Loudspeaker Telephones

2714. "Hands-free" telephones which have built in loudspeakers can act as microphones, passing information from the environment via the telephone system. Such telephones should be removed from conference or meeting rooms, and disconnected when sensitive conversations are being held in their vicinity.

Operations Security

2715. The topic of Operational Security (OpSec) is addressed in more detail at **JSP 440 Volume 1,** but in the context of Audio security it is particularly important to consider OpSec where the subject matter is notionally UNCLASSIFIED, as inferences can be drawn from operator chatter and mannerisms, use of jargon, and call signs.

2716. **Administrative Discussions** Experience has shown that notionally UNCLASSIFIED, administrative discussions concerning such matters as supply problems, technical matters and even social events such as cocktail parties and sports fixtures can be used to provide intelligence on future operational activities, and can also be of interest to terrorist organisations. In particular, where discussions relate to the movements of Senior Officers and VIPs, consideration should be given by originators as to whether a Protective Marking is actually required in order that appropriate security measures are used.

This page intentionally left blank.

COUNTER EAVESDROPPING

This page intentionally left blank.

CHAPTER 28

COUNTER EAVESDROPPING

Scope

2801. Eavesdropping generally refers to the use of listening devices (bugs) in order to overhear, and transmit or record, conversations. This includes long-term devices, perhaps concealed in the fabric of a building, quick-plant devices hidden in a room and certain long-range attack techniques.

2802. Eavesdropping also extends to the practice of attaching covert recording or transmitting devices ("taps") to telephone (or other communications including data) lines within the working area. This subject is addressed in counter eavesdropping because such line-tapping attacks often use the same techniques of surreptitious entry as are used in bugging attacks, and are frequently carried out by the same perpetrators against the same targets; consequently, the countermeasures are very similar. Overhearing of cellphone and personal radio conversations by radio interception is covered in **Chapters 18 and 26** respectively. The collection of unintended electro-magnetic radiation from equipment such as computers is considered in the **Chapter 21**.

2803. The methods, problems and techniques involved in the planting of photographic bugs, (concealed still or video cameras) are essentially the same as those used for audio bugs although the object of the attack will be slightly different. They are less common than audio bugs, but the protective measures are essentially the same.

Threat

2804. The general threat of eavesdropping, and other attacks, is covered in the ***Threat Assessment*** which is issued annually to Principal Security Advisors (PSyA) in TLBs and Trading Funds (TF). COs/HOEs requiring specific threat guidance should initially contact their PSyA who will seek advice from the Joint Security Co-ordination Centre (JSyCC). The elements of the threat which are peculiar to eavesdropping are outlined below:

a. Threats of eavesdropping posed by Foreign Intelligence Services (especially at sites overseas), sophisticated terrorist and subversive organisations and in particular from criminals, investigative journalists, private investigators and some members of the public;

b. The level of threat, as in other areas of protective security, depends upon the attacker's motivation and capability (technical and financial resources and expertise). In the case of eavesdropping, it also depends very largely upon the attacker's ability to gain access to the site of the target conversations;

c. The potential attacker's motivation may be very heavily influenced by his willingness to risk being found out. This risk of discovery and embarrassment is considered high in the UK because of the good protective security regime here. This factor is significant in determining the level of threat of eavesdropping attacks in the UK by a hostile or foreign government. Other groups who do not fear such embarrassment, such as terrorists, criminals etc, may be less inhibited about such attacks ;

d. Overseas, an attacker (especially one with the support of the host government) is likely to be able to achieve a much greater degree of access, and there will be less risk of discovery and embarrassment. Consequently, the threat level is likely to be substantially higher depending on the source of the threat and location of the target;

e. With most forms of security, there is always a significant risk of an "insider" attack, where someone with legitimate access is suborned. This is particularly true in eavesdropping, where access to a room or building can be exploited.

Vulnerabilities

2805. All conversations are vulnerable unless the potential attacker can be denied access to the vicinity of them. The vulnerability relates to the area in which the conversation is being held. The various types of attack can include deliberately planted devices (quickly concealed or deeply embedded in the building), telephone or data-line taps, fortuitous devices (eg accidentally transmitting cellphones), or mains conducting devices. An understanding of the basic principles will help determine the need for appropriate countermeasures.

2806. All devices need a power source and a means of recovering the conversations being collected. The power can be battery or mains electricity, and the device may be remotely switched on and off to conserve power and avoid detection. Recovery of the conversation is often by radio transmission to a nearby listening-post, transmitting down a mains circuit, or a telephone wire or some other feature of the building infrastructure.

2807. Other highly sophisticated techniques include long-distance microphones, laser-eavesdropping and microwave flooding. Such technically advanced and uncommon techniques are not the subject of this general guidance. Further advice on countermeasures to combat these forms of eavesdropping can be obtained from the Security Service through JSyCC, if the threat dictates such sophisticated techniques may be used.

Risk Assessment

2808. It is the responsibility of CO/HOEs to assess the risk of an audio eavesdropping attack in their area using the risk management assessment questionnaire at Annex E to determine a suitable cost effective and risk managed response to the perceived threat. CO/HOEs are to consult their PSyA when assessing the risks to their establishments, and technical security request form (at Annex A) are also to be staffed through the PSyAs. At Annex B are flow charts to be used as a quick look guide in deciding when it is necessary to approach the PSyA for the provision of appropriate countermeasures.

Countermeasures - General

Control Of Access

2809. Good building access controls will be the main deterrent to any potential eavesdropper. Good building design is important, and the incorporation of sensitive zones sited away from vulnerable points (ie adjacent to public areas or toilets, or on ground floor perimeters) is recommended. Staff should be well briefed on the need to prevent unauthorised access; the regime should be supported by suitable pass and access control systems. There should be control and supervision of visitors and staff with limited clearances (eg cleaners, maintenance staff etc).

Control Of Equipment

2810. Measures should be taken to control the introduction by visitors of potentially hazardous electronic devices such as mobile radios, cellphones or various types of recorder, into sensitive areas. Resident staff use of such devices is also to be controlled.

Protection Of Telephone Circuits

2811. Access to communications facilities, telephone exchanges and frame rooms should be restricted to authorised staff. These areas should be secured with appropriate locks when not occupied. Digital telephones are generally more difficult to tap than analogue telephones and should therefore be used in preference to analogue where both systems are *in situ*. However, staff are reminded that as laid down at **Chapter 18**, these telephones **are not secure** for the purposes of protectively marked conversations. Such conversations should only be conducted over approved secure speech telephone systems.

Data Communications

2812. Although computer (or data) communications lines are also digital, they carry greater volumes of information, and thus could be more attractive than telephone

lines. Therefore, protective measures for data lines should include encryption, use of fibre-optic cabling or anti-tamper devices on cabling where the risk of eavesdropping is high. Inspections

Inspections

2813. Counter eavesdropping inspections of sensitive premises may be used to reduce risk where access control measures may have been breached, or to supplement access control measures in areas where the threat is deemed to be high. Inspections are no substitute for good access control measures however. Inspections vary from casual scrutiny of an office by occupants, to simple physical searches and detailed technical inspections (sweeps) by experts. Detailed technical sweeping of government and overseas' sites is usually only carried out by the technical authority as authorised by the Security Service; currently commercial companies are not licensed or authorised to sweep such government/overseas' sites. Some military and other specialised units are trained by the technical authority to carry out limited electronic sweeping at military and other sites both within the UK and overseas. All requests for inspections should be submitted in writing, using the proforma at Annex A to the appropriate PSyA.

Minimum Standard Of Equipment

2814. All trained Service personnel, carrying out Limited Electronic Sweeps (LES), shall have access to the minimum standard of counter eavesdropping equipment as set out in Annex D.

Defensive Radio Monitoring

2815. A mobile radio monitoring unit can be deployed to search for radio transmissions which may be emitted by eavesdropping devices or accidental transmitters. Under the control of the Security Service, it can visit specific UK sites by arrangement, or it can trawl general areas on a random basis. Any requests for the deployment of this equipment should be routed through the relevant PSyA to InfoSy(Tech)

2816. Where significant volumes of protectively marked information are likely to be discussed throughout a building, a permanent automatic radio monitoring system may also be installed, and CO/HOE on sensitive sites will need to be aware of the need to strongly control the installation of radio transmitters in such cases. Before proceeding with a permanent automatic radio monitoring system, PSyAs must consult both InfoSy(Tech) and DCSA CM-CIDA.

General Protection Measures

Buildings

2817. It is reasonable to assume that in general, most sensitive conversations will take place within sites, buildings or rooms which are normally used for processing or storing material up to the same level of protective marking. It therefore follows that sufficient physical, personnel and procedural security measures should already be in place. In most cases within UK, those measures will also provide sufficient counter eavesdropping protection, but where additional measures are required, **Chapter 29** should be consulted.

2818. The principle to bear in mind when considering physical security measures for counter eavesdropping protection, is the prevention of access by attackers to the sensitive area, even when the area is unoccupied and the protectively marked material is safely stored in approved containers. Particular attention must therefore be paid to "out-of- hours" protection (guard patrols, IDS, secured rooms etc).

2819. In addition, it is advantageous to apply certain physical security measures for counter eavesdropping purposes to selected areas or rooms within a building or site (eg some locked offices, IDS for sensitive zones, CCTV, locking of designated conference rooms or briefing facilities). If uncleared personnel are granted access to such areas they should be supervised by appropriately cleared staff and the area re-secured after use.

2820. It may also be necessary (where the threat warrants) to control access to areas adjacent to (including above and below) sensitive rooms in order to prevent casual overhearing and technical attacks which can be carried out from outside the target room.

2821. One of the main justifications for entry and exit searching at access control points is to deter the introduction (by staff and visitors) of equipment which might be used to record or transmit sensitive conversations. This applies mainly to sound recorders (tape recorders, etc) and radio transmitters such as cellphones, mobile radios, portable telephones, etc. Signs should be prominently displayed at access control points of sensitive areas, clearly indicating that such items are prohibited and warning that random searches are conducted

2822. Conference venues and other non-List X commercial premises present difficult problems, because there will be limitations in the application of security. In general it is not advisable to hold prearranged highly sensitive (ie CONFIDENTIAL or higher) discussions (such as conferences) in commercial premises within the UK unless significant measures have been taken to protect those premises in consultation with the relevant PSyA. Overseas, where the threat is higher than in the UK, it is not advisable to hold prearranged discussions in commercial premises above UNCLASSIFIED.

Overseas staff considering higher level discussions at such venues, should consult PJHQ J2X for advice.

Counter Eavesdropping Baseline Measures

2823. A list of specific measures considered appropriate to Very Low threat levels is detailed below. These should be applied in addition to the appropriate physical security measures (as described in **Volume 1 Chapter 5**). The measures below, which are cumulative, should be considered where material of the relevant protective marking is **regularly** discussed. Additional counter eavesdropping countermeasures should be considered whenever the threat to an individual or area is raised. This might be because of media interest, major financial events, evidence or suspicion of information loss through eavesdropping, or for other reasons.

a. **RESTRICTED. Awareness of overhearing.** This will involve promoting security awareness amongst new and existing staff through security lectures on induction and other courses, and awareness material. It will be intended to warn staff not to discuss sensitive matters in public places or where they can be overheard by uncleared visitors, contractors etc.

b. **CONFIDENTIAL. Privacy (closed doors).** This measure requires staff to actively reduce the risk of casual overhearing by closing doors (and windows if necessary) when holding sensitive discussions.

c. **SECRET. Awareness of room contents.** Staff should cultivate an awareness of the room contents so that they are likely to detect changes or new items appearing in the rooms overnight or after visitors have left. A clear-desk policy can help to achieve this.

d. **TOP SECRET. Casual search by room occupants.** Rooms regularly used for TOP SECRET conversations should be periodically subjected to a casual search for suspicious objects. This should be done by someone familiar with the room, though not necessarily trained or experienced in counter eavesdropping searching.

N.B. These are additional to physical security baseline measures.

General Counter Eavesdropping Awareness

2824. General counter eavesdropping awareness can be achieved by a brief session on counter eavesdropping during staff security lectures, or by means of other education and awareness material (e.g. posters, films). It should be aimed primarily at those staff most likely to be at risk of attack.

Access To Telephone Exchanges

2825. Access to telephone exchanges, frame rooms and distribution boxes should be restricted to authorised staff. Telephone frame rooms are to be secured with appropriate locks when not occupied and distribution boxes locked or sealed except when access is needed. Visiting maintenance staff and contractors are to be security cleared or their access strictly controlled and their work supervised within such areas.

Increased Counter Eavesdropping Awareness

2826. Increased counter eavesdropping awareness should be achieved through attendance on counter eavesdropping awareness or training courses. This should be provided to security staff responsible for sensitive areas.

Technically Inspected (Swept) Rooms

2827. Rooms where sensitive discussions take place regularly (such as meeting or conference rooms), and which have been "swept" for eavesdropping devices, are to be locked when not in use and the keys controlled out of duty hours. Details for safeguarding such rooms are given in Annex G.

Digital Telephones

2828. Digital telephones are significantly more difficult to tap than analogue telephones and should therefore be used wherever appropriate. Approved secure telephones do, of course, supply significantly more protection against tapping.

Control Of Voice-Processors

2829. Voice-processing boards in personal computers (PCs) can malfunction or be tampered with to act as microphones in rooms, and can store or transmit eavesdropped conversations. Unless operationally necessary, such features should be physically disconnected by a competent person.

Control Of PA Systems

2830. PA speakers inside a sensitive room can readily be adapted to act as microphones if access can be gained to the PA system wiring elsewhere. Where access to this wiring is not fully controlled, consideration should be given to siting speakers outside sensitive rooms. Safety must not be compromised of course, and technical measures may need to be applied to isolate speakers which must remain in sensitive areas.

Control Of Loudspeaker Telephones

2831. "Hands-free" telephones which have built in loudspeakers can malfunction to act as microphones, accessible via the telephone wiring or telephone system. Such telephones should be removed from conference or meeting rooms, and disconnected when sensitive conversations are being held in their vicinity. Alternatively, such features should be disabled, or other technical measures applied to ensure they cannot be subverted.

Control Of Recording Equipments

2832. As well as static installations such a conference room dictation systems, a number of portable items which may be fitted with microphones and a recording capability are liable to be brought into defence premises. This includes a number of models of Handheld CIS such as Personal Digital Assistants (PDA) that may have been approved for official use under the regulations laid down at **Chapter 8**, some models of mobile telephones that may have been approved for official use under the regulations laid down at **Chapter 18**, and ancillary items such a personal audio equipments (including compact cassette (CC), MiniDisc (MD) and RAM (MP3) based systems) and toys such as *Furbys*.

2833. Where official PDAs and mobile phone are to brought into sensitive areas, care must be taken that their recording facilities cannot be accidentally activated by the holder, or remotely activated. Ancillary recording equipments may only be brought into sensitive areas by the approval of the appropriate local security staffs.

Inductive Loops

2834. As well as the direct audio signal, it is also possible for an attacker to exploit the inductive loops fitted to various types of equipments to aid those with hearing disabilities. If any equipment fitted with such facilities is to be intalled on a defence site, the Co-ordinating Installation Design Authority (CIDA) as laid down at **Chapter 17** should be consulted.

Acoustic Hoods

2835. Acoustic hoods offer some privacy in general office areas, but must be sited carefully to be effective.

Secure Speech Enclosures

2836. Secure speech enclosures offer a high degree of privacy. Their use should be considered where sensitive discussions take place in a high risk environment, and when using approved secure speech systems in such environments.

Physical Search

2837. Periodic physical searches by security staff (usually security guards in MOD civilian establishments and trained service personnel in service establishments) are an effective countermeasure against quick-plant devices. Basic guidelines for carrying out a physical search can be found at Annex C. Advice on training in physical searching is available through the relevant PSyA.

Rotation Of Telephones

2838. Rotation of telephones is an effective and low-cost method of reducing the risk of bugging of the telephones of particular prominent targets. Phones are redistributed amongst users at intervals (eg six monthly), possibly via a central pool. However, it is important to ensure that rotated telephones are checked for eavesdropping devices **before** they are passed on to a new user.

Limited Electronic Sweeps (LES)

2839. A limited form of technical search (sweeping) is practised by some military and other specialised units. LESs are usually confined to military or other specific sites both within the UK and overseas. Requests for an LES should be submitted to the appropriate PSyA, by completing the proforma at Annex A. PSyAs will coordinate LESs within their area of responsibility. If there is doubt as to which Sector has the lead responsibility at a joint Service establishment within the UK advice is to be sought from InfoSy(Tech). In the event of uncertainty concerning the lead Service responsibility at joint establishments overseas, advice is to be sought from PJHQ J2X.

2840. Where feasible, the specialised units shall provide technical assistance to any unit or establishment, whether military or civilian, whose own PSyA is unable to carry out the requested LES. Costs for LESs will be borne by the TLB or TF, as appropriate.

Technical Security Survey (TSS)

2841. At sites where physical, personnel and procedural security is high, and in line with a LOW threat, a Technical Security Inspection (TSI) is not justified. In the case of a large building complex, where a TSI is not practical, a TSS, carried out by a team of counter eavesdropping experts under the control of the relevant PSyA, may be used to assess vulnerability to eavesdropping attack.

Tamper Proofing

2842. Tamper proofing, or tamper-detection of equipment (telephones, answerphones) and related infrastructure (telephone sockets, junction boxes, mains sockets, extension cables and multi-sockets etc) may detect replacement or tampering. This can be achieved by seals, details of which are given in **Volume 1 Chapter 5**.

Technical Security Inspection (TSI)

2843. A TSI is an in-depth technical inspection (sweep) to search for clandestine devices by a team of experts from the technical authority. TSIs can be implemented at high-risk sites, provided that the integrity of the site can be maintained. This facility can also be put into operation where an attack is strongly suspected. Requests for TSIs should be arranged through the appropriate PSyA, by completing the proforma at Annex A. Costs for TSIs will be borne by the TLB or TF, as appropriate, and the periodicity and depth of inspections should be agreed with InfoSy(Tech).

Action To Be Taken When An Eavesdropping Device Is Found

2844. Search teams who believe they have found an eavesdropping device in an office/conference room etc should immediately follow the guidance given at Annex F.

CONFIDENTIAL (when completed)

ANNEX A

MINISTRY OF DEFENCE TECHNICAL SECURITY REQUEST FORM

1. UNIT/ESTABLISHMENT	**2. ADDRESS (including Post Code)**
3. BUILDING NAME (if any)	**4. ROOM NO(S)**
5. NAME OF POINT OF CONTACT FOR ADD'L INFORMATION	**6. RANK/GRADE**
7. FULL TELEPHONE NUMBER	**8. TYPE OF SERVICE REQUIRED (TSI/LES/PHYSICAL SEARCH/ON-GOING ADVICE AND ASSISTANCE/PRE-CONSTRUCTION ADVICE/OTHER)**
9. ACCESS AND CLEARANCE REQUIRED BY TECHNICAL AUTHORITY TO ENTER DESIGNATED AREA	**10. NUMBER OF TELEPHONE IN DESIGNATED AREA**
11. SQ METRES (APPROX) OF DESIGNATED AREA (ATTACH PLANS, IF AVAILABLE)	**12. HIGHEST PROTECTIVE MARKING DISCUSSED/PROCESSED IN DESIGNATED AREA**

CONFIDENTIAL (when completed)

CONFIDENTIAL (when completed)

13. FREQUENCY OF USE AT LEVEL STATED IN BOX 12 ABOVE:	**14. RISK MANAGEMENT ASSESSMENT ATTACHED: YES/NO**
15. REMARKS	
16. SIGNATURE OF PERSON REQUESTING SERVICES	**17. SIGNATURE OF USO/BSO**
18. APPROVED/REJECTED BY PRINCIPAL SECURITY ADVISOR (GIVE REASONS FOR APPROVAL/REJECTION) **SIGNED BY:** **NAME:** **RANK:** **BRANCH/DIRECTORATE**	

CONFIDENTIAL (when completed)

ANNEX B

CHART TO ASSESS POSSIBLE REQUIREMENT FOR COUNTER EAVESDROPPING MEASURES WITHIN THE UK

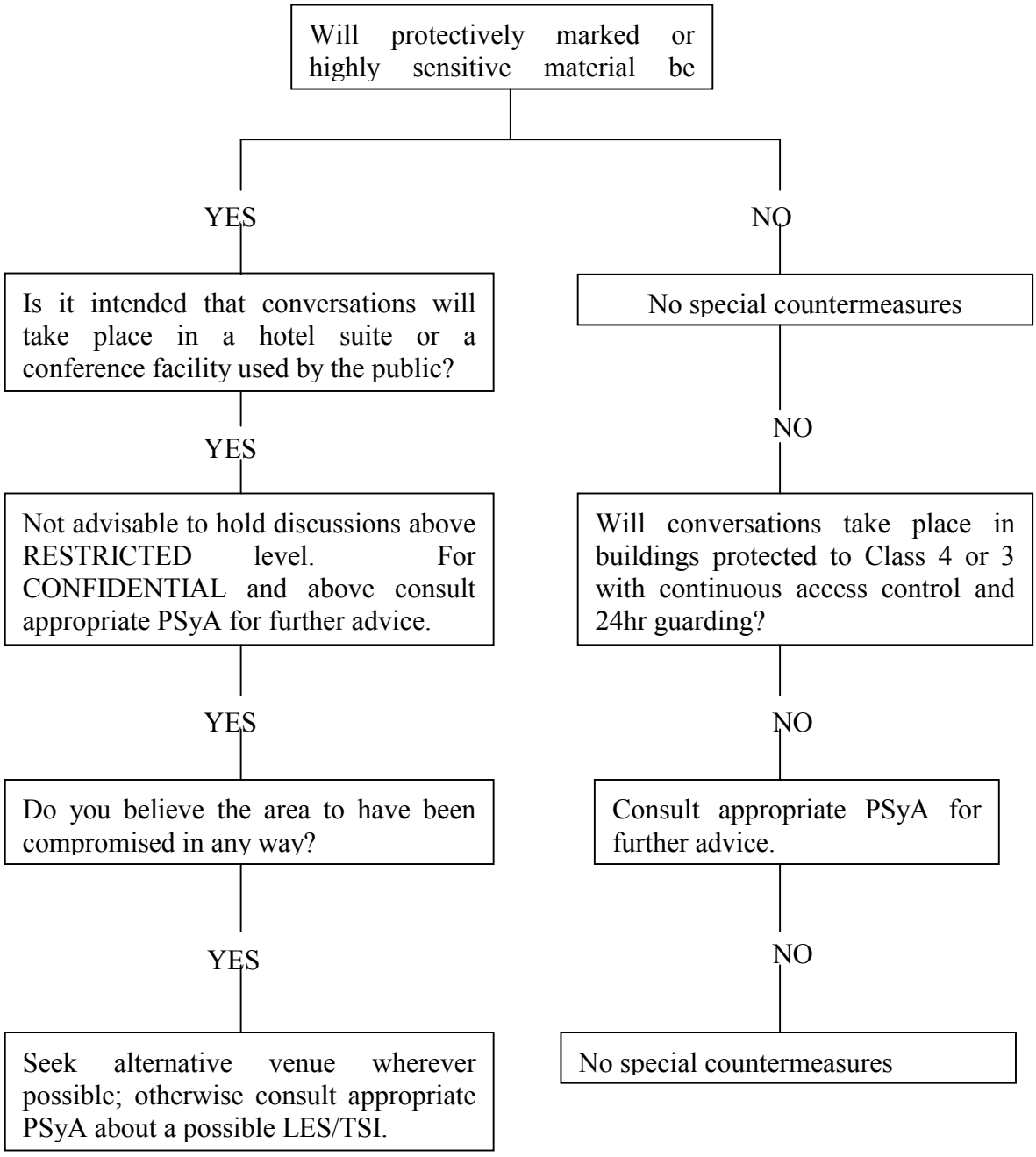
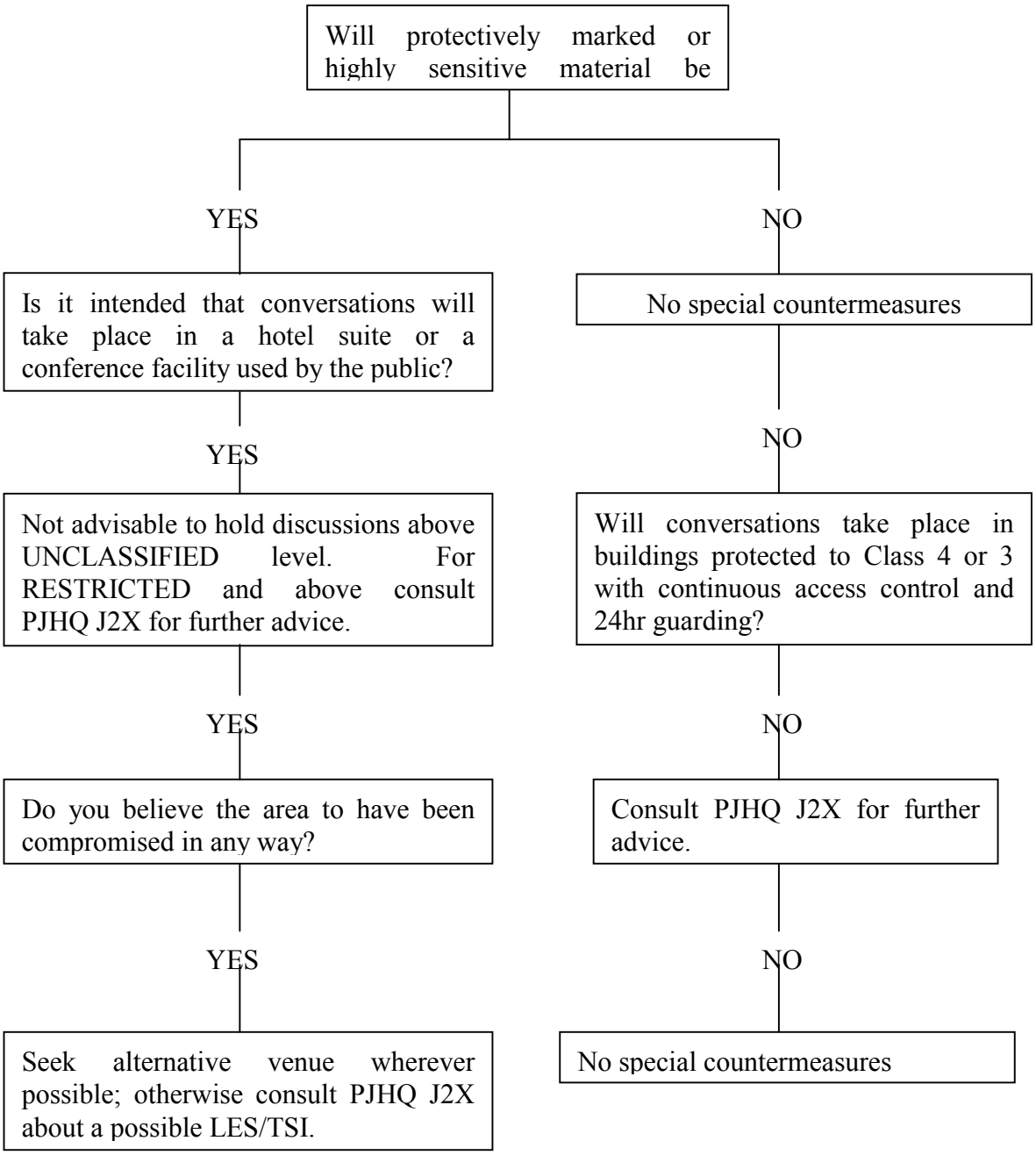


CHART TO ASSESS POSSIBLE REQUIREMENT FOR COUNTER EAVESDROPPING MEASURES OVERSEAS



ANNEX C

PHYSICAL SEARCHES FOR EAVESDROPPING DEVICES

Physical search

1. Physical searches, by properly counter eavesdropping trained security staff, are an effective countermeasure against quick-plant devices. Searches should be considered after uncleared visitors or intruders are thought to have had access to sensitive areas. They should also take place periodically in sensitive areas. The search can be split into 3 phases.

Phase 1 - Before the search

2. Before the search is started, the searcher (or searchers) should:

a. Plan how the search is to be conducted (ie systematically from an agreed start point within the room), and the features to be checked (furniture, wall, ceiling and fitments). Each member of the team should know which area of the room they are responsible for.

b. Obtain searching tools (steps, screwdrivers, torches and mirrors).

c. Where possible, consider how long an attacker would have had access to the room. The less time an attacker has access to an area, the more chance there is that the device will be a "quick plant type" or a device superficially hidden in something common to either an office or the room generally (eg plug adaptor or ornament).

d. Make arrangements for preventing interruptions during the search (eg lock the door).

e. Keep knowledge of the search to the minimum number of staff with a real need to know.

f. Establish what action is to be taken if anything is found (see Annex G).

Phase 2 - Procedures

3. The following procedures should be adopted when conducting a physical search for eavesdropping devices:

a. Lock the door and commence the search working in accordance with the plan.

b. The search should be carried out in silence. Starting at an agreed point and systematically working around the room.

c. Pay particular attention to any changes which you believe have been made since any previous search (eg new furniture and furnishings).

d. When checking furniture such as bookcases and tables, look for indications that a device may have been removed before the search (eg traces of holes, scratch marks or adhesive tape).

Common areas of concealment

4. Some common areas of concealment are:

a. **Chairs.** Check chairs thoroughly, looking at the underside, back, arms and in recesses covered by furnishing material. It is possible for an attacker to carefully slit a material cover and insert a device into a padded area of a chair. Cushions should be removed and inspected separately.

b. **Tables, desks, bookcases and cabinets.** Remove any drawers or shelves from units which are not locked and inspect them thoroughly, then inspect the drawer or shelf cavity of the unit. Check all surfaces beneath and on the sides of units. Look for indications of concealed compartments. You should satisfy yourself that all surfaces, including those not fully visible, are free of devices and traces.

c. **Ornaments etc.** Books, clocks, pictures, vases and ornaments should be carefully inspected.

d. **Wooden fitments.** Examine door frames, doors, windows and window frames, ledges, pelmets, panelling, mouldings and skirting boards for evidence of loose sections or places of concealment.

e. **Curtains.** Heavy curtains with loose lining can act as excellent receptacles for concealed devices. Check a curtain with a lining by spreading it across the window, pulling up the bottom hem and separating the lining from the curtain to peer up to the top. It may be advisable to use a torch to see to the top, as many devices are coloured black. Finally check the curtain runners before running hands down the full length of the curtain, paying particular attention to the edges for odd lumps or bumps.

f. **Furnishings.** Examine cushions, loose covers, carpeting etc to identify

places that could be used to hide devices.

g. **Electrical equipment.**Electrical equipment (eg computers, telephones and desk lamps) should be examined externally but should not be taken apart without qualified supervision.

h. **Electrical fittings.** Electrical fittings (eg sockets, light switches etc) should be closely examined for any signs of tampering, but not opened without qualified supervision.

i. **Telephone sockets and junction boxes.** Telephone sockets and junction boxes should be visually checked with the covers removed but they should not be interfered with, without qualified supervision.

j. **Other places.** Inspect areas behind radiators, water pipes, in conduits, in and around ventilator shafts and ducts. Check suspended ceilings and floors, removable wall panels, window blinds etc.

What to do if a device is found

5. Full details are given in Annex F, but the following is a brief summary of the action to be taken if a device is found:

a. Do not discuss the find in the room concerned;

b. Do not touch the device, leave it in place;

c. Secure the room when you leave it;

d. Report to the Joint Security Co-ordination Centre (JSyCC), through your PSyA, as soon as possible.

Phase 3 - What to do after a search has been carried out

6. After the search:

a. The search team should be debriefed by the search coordination supervisor to ensure that all the areas have been inspected adequately and any suspicious objects investigated.

b. For rooms where sensitive discussions take place, and the room is searched periodically, check on the arrangements for controlling access, and the security of the door keys (including duplicates). Where the search has taken place prior to a conference, access should be controlled until the conference is complete.

c. If the room has been searched prior to a conference, ensure that any furniture, ornaments, flowers etc brought into the room before the conference are examined, and nothing extra is brought in after the search.

ANNEX D

MINIMUM STANDARD OF EQUIPMENT REQUIRED FOR A LIMITED ELECTRONIC SWEEP (LES)

1. The object of an LES is to detect an eavesdropping device. If such a device **is** found during an LES, it should be left untouched and the guidance in Annex F followed. The more simple the LES can be kept, the more cost effective it will be. Therefore only equipment necessary to counter the threat should be used. That equipment should be simple to use, easy to deploy and require little, or no detailed analysis.

2. Before purchasing any new and expensive equipment, the LES authority should determine the types of eavesdropping attack likely to be encountered and purchase the appropriate equipment. The following is a list of the type of equipment that **may** be required by an LES team to fulfil its duties, giving specification parameters approved by the technical authority.

a. **Technical search unit**

This should be capable of:

(1) monitoring for line borne audio signals in the frequency range 300Hz to 12kHz on mains, telephone or computer wiring. It should be capable of monitoring on either the LIVE or NEUTRAL line relative to earth;

(2) a tuned radio frequency (RF) unit capable of detecting line borne RF signals in the frequency range 10kHz to 30MHz on mains, telephone or computer wiring; and

(3) a wide band radio receiver designed to detect spatial irradiations in the frequency band 30MHz to 1GHz.

b. **Scanning receiver**

This should be capable of scanning for, and locking on to, spatial transmitters operating in the frequency range 10MHz to 2GHz. It should be easy to operate and have a demodulating facility to aid signal identification. If considered necessary, a second scanning receiver could be used to extend the frequency coverage to 4GHz.

c. **Non-linear junction detector (NLJD)**

This equipment is only considered necessary if you require a portable harmonic radar capable of detecting non-linear devices, active or inactive, concealed in walls, cavities or ceilings etc. It should be capable of discriminating against false responses such as those produced by nails, screws and wire mesh etc. Modern commercial NLJDs are easy to use and can be a useful edition to an LES team's kit. However, it should be borne in mind that any response gained using a NLJD must be investigated and eliminated. A NLJD will respond to many items including, for example, telephones and computer terminals **in adjacent rooms**.

ANNEX E

RISK MANAGEMENT ASSESSMENT OF POSSIBLE EAVESDROPPING ATTACK

1. **List valuable assets eg:**

   a. TOP SECRET Codeword discussions (operational, tactical, SIGINT etc).

   b. CONFIDENTIAL or SECRET discussions (operational, tactical, SIGINT etc).

2. **Determine assets value (ie impact of compromise of an asset):**

   a. TOP SECRET: The compromise of this information is likely to:

      (1) threaten directly the internal stability of UK and friendly countries;

      (2) lead directly to widespread loss of life;

      (3) cause exceptionally grave damage to effectiveness or security of UK or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations; or

      (4) cause exceptionally grave damage to relations with friendly governments.

   b. SECRET: The compromise of this information is likely to:

      (1) raise international tension;

      (2) damage seriously relations with friendly governments;

      (3) threaten life directly or individual security or liberty; or

      (4) cause serious damage to the operational effectiveness or security of UK or allied forces or the continuing effectiveness of highly valuable security or intelligence operations.

   c. CONFIDENTIAL: The compromise of this information is likely to:

      (1) materially damage diplomatic relations (ie cause formal protest or other sanction);

(2) prejudice individual security or liberty;

(3) cause damage to the operational effectiveness or security of UK or allied forces or the effectiveness of valuable security or intelligence operations.

3. **Identify possible threats to your site, such as from:**

a. Foreign Intelligence Services.

b. Terrorist groups.

c. Disaffected staff.

d. Criminals.

e. Investigative journalists.

4. **Identify vulnerabilities of the site/area concerned (to be carried out in conjunction with Establishment Security Officer):**

a. Is interception of sensitive discussions (using bugging devices) likely? (If no, do no more).

b. Is there good access control?

c. Are there effective security measures in operation around the perimeter of the site (eg secure fencing, CCTV etc)?

d. Are there effective physical security measures in operation within the site (eg IDS, 24hr patrols, secure rooms, etc)?

e. Are there effective personnel security measures in operation within the site (eg escorting uncleared visitors, vetting and supervision of relevant staff etc)?

f. Are there effective communications and technical security measures in operation within the site, such as:

(1) a ban on all mobile phones, radio equipment etc being brought into controlled areas;

(2) checks carried out periodically for tampering (eg traces of holes, scratch marks etc);

(3) strict control of entry to the site telephone exchange, frame room and junction boxes;

(4) vetting of telephone engineers or escorting within telephone exchange/frame room;

(5) control of telephones (eg digital, analogue and secure) and data facilities on site;

(6) control of telephone loudspeaker and external microphone facilities (eg they are inhibited and/or brought to the attention of users through telephone security orders/labels?);

(7) standard office equipment (eg computers, photocopiers, fax machines etc) maintained by an accredited agency (eg supplier or repair facility on approved government contract);

(8) is any standard office equipment installed that has a remote diagnostic facility;

5. **Review existing security countermeasures against eavesdropping attacks and implement necessary changes.**

Stage 1 - Review existing security countermeasures

a. Do staff receive adequate education in the application and relevance of counter eavesdropping measures?

b. Are the physical security baseline measures laid down in JSP 440, Volume 1, Chapter 5 adhered to?

c. Are the mandatory standards for protection against eavesdropping laid down in JSP 440, Volume 3, Chapter 28 adhered to?

Stage 2 - Decide whether changes need to be implemented.

d. Having reviewed existing security countermeasures and the standards of security imposed on the site, you should decide whether they are:

(1) excessive;

(2) adequate; or

(3) inadequate

in relation to the threat of an eavesdropping attack.

e. If excessive, consider whether funding or resources can be saved by sensibly reducing them whilst still maintaining the desired level of security.

f. If adequate, do no more.

g. If inadequate, then the assets are at an unacceptable degree of risk. A decision is required on what to do to reduce the risk to an acceptable level.

6. **Total security review (To be carried out by security staff)**

Conduct a general review of countermeasures against threats and vulnerabilities to ensure that the overall result meets mandatory standards, is cost effective and that the Head of Establishment is prepared to accept any remaining residual risk. Also ensure that the key facts and decisions in the risk management analysis have been recorded to enable audit in the future.

ANNEX F

ACTION TO BE TAKEN ON DISCOVERY OF AN EAVESDROPPING DEVICE

Principal

1. All "finds" of eavesdropping devices, which relate to government information or premises, must be immediately reported through the chain of command to the DSO via the Joint Security Co-ordination Centre (JSyCC). This Annex should be brought to the attention of all personnel likely to be involved in physical searches and electronic sweeps.

On Discovery

2. If a suspicious object is identified as an eavesdropping device, make no comment. Do not tamper with or attempt to remove the suspect device. Advise the remainder of the team by a written note to withdraw from the room. Secure the room and report to the local security staffs immediately.

3. Persons knowledgeable of the incident must be kept to an absolute minimum, to protect innocent individuals and investigative efforts.

4. The local security staffs should inform the appropriate PSyA, by secure means immediately. If the incident occurs outside of normal duty hours then information should be directed to the appropriate PSyA Duty Officer where one exists, or in other cases direct to the JSyCC.

Escalation Procedure

5. Guidance must be sought from the Security Service through the JSyCC before any further action is taken.

Post-find investigation

6. A post-find investigation is necessary when an eavesdropping attack is discovered in order to attempt to determine the identity of the attackers and recommend any remedial action.

7. Since the find of any eavesdropping device is *prima facie* evidence of a criminal offence having occurred, investigations should normally be carried out by a team consisting of the PSyA, the Ministry of Defence Police (MDP) or Service Police as appropriate as the evidential authority, and representatives of the Security Service along with any technical agency they may deem necessary to provide support.

8. Details of the investigation, once completed, are to be furnished to the DSO via the JSyCC.

ANNEX G

SAFEGUARDING TECHNICALLY INSPECTED (SWEPT) ROOMS

1. The person responsible for a swept room shall be appointed by the CO/HOE or head of branch/unit as appropriate. The person selected must hold a DV clearance.

2. All doors to a swept room shall be fitted with security approved locks.

3. When the room is unoccupied the doors shall be kept locked.

4. No more than two keys are to be cut for locks to doors of swept rooms. One key is to be retained by the local security staffs, for use in an emergency, the other by the appointed person responsible for the room. The key(s) must never be left unattended in the lock or be taken out of the building/off the site. The key(s) must be kept in a secure container fitted with an approved combination lock when not in use. The keys are to be included in the six monthly check of security keys laid down in **Section XII to Chapter 5 of Volume 1**.

5. No unauthorised person shall be allowed in a swept room unless supervised by appropriately cleared staff at all times.

6. The person responsible for the swept room should seek the advice of Sector security staff, as appropriate, through the local security staffs before any works services are carried out in a swept room.

7. The person responsible for a swept room shall maintain a security log book (MOD Form 931) showing the following details:

   a. the name(s) of the person responsible for the room;

   b. all visitors who enter the room;

   c. all works services carried out in the room;

   d. all furniture and equipment installed in the room, including items removed and returned after repair.

8. The security log book should be periodically examined by the local security staffs and may be inspected by the appropriate PSyA at any time.

9. No additional furniture or equipment of any kind shall be moved into a swept

room until the item has been examined and approved by appropriate security staff. When furniture or equipment is sent away for repair, or temporarily stored elsewhere, the fact that it came from, or may return to, a swept room should not be disclosed.

10. All staff should be made aware that eavesdropping devices can be extremely small and may be planted in a wide range of products.

11. Any circumstances which suggest that a swept room may have been compromised should immediately be reported to the ocal security staffs and the guidance given in Annex F followed.

12. The above guidance is to be followed if the integrity of the swept room is not to be compromised.

INTRODUCTION TO STRUCTURAL ACOUSTIC PROTECTION

This page intentionally left blank.

CHAPTER 29

INTRODUCTION TO STRUCTURAL ACOUSTIC PROTECTION

Introduction

2901. In cases where a high volume / frequency of discussions of material attracting a protective marking are likely to occur in an MOD establishment, it may be necessary to consider ways in which building structures can be augmented to protect information when carried in an acoustic (sound) form.

Assessment

2902. When planning the construction of a new facility, the relocation of staff, or a new or changed role, Project Managers should seek to determine the like volumes and frequencies of discussions that will take place above RESTRICTED.

2903. Where no information protectively marked above RESTRICTED will be discussed, the Audio security measures described in **Chapter 27** should suffice.

2904. Where information protectively marked at CONFIDENTIAL will be discussed regularly, or where SECRET or TOP SECRET will be discussed occasionally, the general protection measures described in this Chapter should be considered, and **Chapter 28** should be reviewed for Counter Eavesdropping considerations. The relevant Principal Security Advisor (PSyA) should then be approached for advice before any plans are finalized.

2905. Where information protectively marked at SECRET or TOP SECRET will be discussed regularly, or where Compartmented (e.g Codeword) material will be discussed occasionally, there may be a need for the special protection measures described later in this Chapter. The Counter Eavesdropping considerations of **Chapter 28** must also be reviewed, and the relevant PSyA must then be approached for advice before any plans are finalized.

General protection measures

2906. It is reasonable to assume that in general, most sensitive conversations will take place within sites, buildings or rooms which are normally used for processing or storing material up to the same level of protective marking. It therefore follows that sufficient physical, personnel and procedural security measures should already be in place. In most cases within UK, those measures will also provide sufficient acoustic protection.

2907. The principle to bear in mind when considering physical security measures for acoustic protection, is the prevention of access by attackers to the sensitive area. If uncleared personnel are granted access to such areas they should be supervised by appropriately cleared staff.

2908. It may also be necessary (where the threat warrants) to control access to areas adjacent to (including above and below) sensitive rooms in order to prevent casual overhearing which can be carried out from outside the target room.

2909. One justifications for entry and exit searching at access control points is to deter the introduction (by staff and visitors) of equipment which might transmit sensitive conversations, such as cellphones and mobile radios. Signs should be prominently displayed at access control points of sensitive areas, clearly indicating that such items are prohibited and warning that random searches are conducted.

2910. Conference venues and other non-List X commercial premises present difficult problems, because there will be limitations in the application of security. In general it is not advisable to hold prearranged highly sensitive (ie CONFIDENTIAL or higher) discussions (such as conferences) in commercial premises within the UK unless significant measures have been taken to protect those premises in consultation with the relevant PSyA. Overseas, where the threat is higher than in the UK, it is not advisable to hold prearranged discussions in commercial premises above UNCLASSIFIED. Overseas staff considering higher level discussions at such venues, should consult the PJHQ PSyA for advice.

Special protection measures

2911. The exact measures required where information protectively marked at SECRET or TOP SECRET will be discussed regularly, or where Compartmented (e.g Codeword) material will be discussed occasionally, are currently under review. Where such advise is required in the interim, InfoSy(Tech) should be approached through the PSyA for case-by-case advice.

ACOUSTIC EMISSION SECURITY

This page intentionally left blank

CHAPTER 30

ACOUSTIC EMISSION SECURITY

Introduction

3001. Acoustic emissions are used in the maritime environment by sensors (e.g. sonar), communications systems, and decoys. The presence of these emissions in the environment can present potential security issues in terms of Confidentiality, Integrity and Availability.

3002. The security of data deliberately modulated upon acoustic emissions is covered within the Communications Security (COMSEC) discipline, typically by the use of cryptographic systems, as laid down at **Chapter 23**.

3003. Acoustic Emission Security is defined as those measures taken to prevent interception and exploitation of those intentional acoustic emissions not produced specifically for communications purposes. It is analogous to the discipline of Electronic Emission Security (ELSEC) for Radio Frequency issues as detailed at **Chapter 21, Section 2**.

3004. The nature of the threat environment means the current requirements for Acoustic Emission security measures deal only with the countering of Intelligence gathering activities by a hostile group or country.

Overview

3005. The interception of acoustic emissions can be an attractive and profitable source of intelligence, as it can in principle be undertaken from the safety of home territory; international air space; or the high seas. Such interception could reveal information relating to certain aspects of the electronic techniques employed within the equipment or the extent and preparedness of the country's defences, which is otherwise protected by physical, personal and CIS security measures.

3006. The aim of Acoustic Emission Security practices is to minimise, as far as possible, the risk of emission information being compromised (that would in itself be protectively marked) by limiting the opportunities for its interception by any hostile group or country. Total denial is impracticable in most cases without seriously impeding the progress of a project through its developmental stages and more so when operational. Acoustic devices by their nature will emit, the aim of security is to assess the risk and implications of compromise by interception and then to apply protective measures commensurate with protective marking, the characteristics of the emission, and the local conditions.

3007. The protective marking associated with information obtainable from interception of acoustic emissions is generally considered to be higher in the early stages of research and development. Although it may not be practicable to maintain the same degree of security from the beginning of the development of an item of equipment to the in-service date and beyond, continuation of security is essential.

3008. The technical analysis of such emissions can provide data which can be used against MOD platforms, and/or may allow development of similar equipment or systems. These may involve sophisticated deception and decoy techniques or jamming. Indeed successful interception and analysis could allow the development and deployment of countermeasures to coincide with the operational use of the target signals.

3009. The intercept of only seconds of a complex signal can provide vital information as to its purpose, modes and technical characteristics. Generally speaking, a high signal level is necessary for analysis but even at low level this will alert an interceptor to a signal of interest and for a subsequent attempt at intercept he/she can then maximise resources. Weaknesses or exploitable features, which may not be evident to the developer, may give hostile analysts an early lead in designing countermeasures.

3010. The main system types for which acoustic emissions will need to be considered are as follows:

a. Sonars ;

b. Beacons and Navigational aids ;

c. Torpedo Guidance and Control ;

d. Targets and Decoys ;

e. Fuzing Systems.

3011. In providing protection for the emissions listed, consideration must also be given to the security of any communications associated with their testing, servicing and operation, in accordance with **Chapter 23**.

Responsibilities

3012. UK national security policy is the responsibility of a Cabinet Office Committee (SO), who hold the authority to advise on the implementation of this policy, having liased with the Security Services and other appropriate authorities responsible for both assessing the overall threat and advising on the need for countermeasures.

3013. Overall responsibility for assessing the threat, vulnerability, and risk, lies with the MOD Security Authority, Sy(Pol)2c, on the staff of the Departmental Security Officer (DSO), and is implemented through the security chain of command.

3014. Responsibility for the selection of countermeasures for individual systems lies with Project Managers and/or System Operating Authorities (SOA), the individual threat assessment process is however a matter purely for the security authority.

3015. **Defence Intelligence Staffs (DIS).** The DIS is responsible for production of information relating to the current Acoustic Emission Threat.

Risk Assessment

3016. A risk assessment is to be carried out early in the planning stages of a project in order to minimise any subsequent impact on design and cost caused by Acoustic Emission considerations. A similar exercise will need to be conducted when modifications to existing equipment are proposed.

3017. The risk assessment will comprise of a review of the asset value, the generic and local threats, and the vulnerabilities.

3018. **Information Value** The sensitivity of an emission may be gauged from the classification assigned to the project:

a. RESTRICTED : Intercept and exploitation would be undesirable ;

b. CONFIDENTIAL : Intercept and exploitation would be dangerous ;

c. SECRET : Intercept and analysis would cause serious injury ;

d. TOP SECRET : Intercept and exploitation would normally cause exceptionally grave danger.

3019. **Threat** Acoustic Emission attacks are expensive in resources, difficult to mount, and unpredictable in outcome. They are therefore likely to be attempted only where all the following circumstances are met:

a. Other methods of intelligence gathering are impractical ;

b. An attack is practical (i.e. the attacker can acquire a position close enough to the radiating equipment and from which he/she can operate undetected over an extended period).

3020. DIS issues specific warnings by formal signal message of any short-term changes to the threat environment, such as the presence of known collection platforms (typically AGIs) within UK territorial waters.

3021. **Vulnerabilities** The likelihood, or risk, of a successful attack will depend on the extent of the perceived threat to an installation, together with the Acoustic Emission vulnerabilities of the equipment or system involved (i.e. its propensity to radiate).

Countermeasures

3022. The detail and amount of effort required for protection of both intentional and unintentional emissions of each system are to be assessed by considering the following key factors :

a. Purpose and sensitivity of emission ;

b. Risk of emission compromise in its specific environment.

3023. The following baseline countermeasures can be assumed to be required in all cases, be it for the development, production or maintenance stages of a system's lifecycle.

3024. Careful planning of tests and trials:

a. Avoidance of forewarning of tests and trials ;

b. Variation of times of day and, where possible, of intervals between tests and trials ;

c. Reduction to the essential minimum of the:

(i) time during which the equipment operates ;

(ii) power required ;

(iii) combination in one test or trial of different operational modes of one type of equipment.

d. Receipt and review of DIS warning messages for any short-term environmental issues.

Incident Handling

3025. Actual or suspected compromises of Acoustic Emissions must be reported, as with all other Information Security concerns, in line with the requirements of **Chapter 11**.

DEPARTMENTAL SECURITY OFFICER

GUIDANCE NOTES

Intentionally blank

D/Def Sy 1/9
August 2001

DEPARTMENTAL SECURITY OFFICER
GUIDANCE NOTE No 1

Security Responsibilities post Security Structures Review

Introduction

1. This Guidance Note describes the organisation, management and delivery of security in the MOD following the Security Structures Review (SSR). It sets out the delegations to Top Level Budget (TLB) Holders and Chief Executives of MOD Trading Funds (TFCEs), and the revised responsibilities of organisations and staff involved in determining security policy, those implementing policy, and those providing security support advice and assistance.

2. TLB Holders remain responsible for implementation of security measures in those Vote funded Defence Agencies for which they, or their senior staff, are Owners. Trading Fund Agencies will for security assurance purposes be treated in the same way as TLB Holders, and be held accountable to the Departmental Security Officer (DSO).

3. Separate guidance is being issued on revised responsibilities for dealing with the security of nuclear weapons and nuclear materiel.

Background

4. The Strategic Defence Review (SDR) of 1998 led to significant changes in the way the business of the department is conducted. As a result, in September 1999, 2nd PUS commissioned a review to examine the organisation of security in the department. This review – the Security Structures Review (SSR) – was to consider all aspects of security except policing, guarding and vetting. The results of the review were endorsed by the Defence Management Board on 25 January 2001 as DMB (00) 12. DCI 148/01 reported the outcome.

Impact of SSR

5. A guiding principle of the SSR was that security is a core business issue and should be firmly embedded in management systems and processes of the Department with ownership of risk unambiguous, and aligned with budgetary authority and accountability. It is the responsibility of everyone working in the Department. The management of security risk is to complement and mirror the application of corporate governance principles.

6. The main elements of the revised security structure are as follows:

a. **Responsibilities in the Ministry of Defence**. Overall responsibility for security in the MOD rests ultimately with the Defence Council. PUS is a member of the Official Committee on Security (SO), the senior Cabinet Office Committee for security matters, responsible for formulating HM Government policies on all aspects of security and co-ordinating their application. The Director General Security & Safety (DGS&S) is the DSO responsible for overseeing the implementation and dissemination of protective security policy, the issue of guidance and for incident reporting. The DSO also contributes to the formulation of national security policy and is a member of SO sub committees dealing with information security (SO(IS)), and protective security (ICPS). As part of the process of security assurance required under corporate governance, DGS&S is required to submit an annual Certificate of Assurance to the Defence Audit Committee (DAC).

b. **Directorate of Defence Security.** A single headquarters policy and standards-setting division, the Directorate of Defence Security (DDefSy), formed on 1 April 2001 reporting to the DSO. This new division has been formed from the former Directorate of Security Policy (DSy(Pol)) and policy elements dealing primarily with industrial security matters and scientific and technical security advice from the former DHQSy division. The Directorate's responsibilities are at Annex A. These include responsibility for the newly created Joint Security Co-

ordination Centre (JSyCC) to co-ordinate alerts and warnings of information security incidents, including electronic attacks. The JSyCC will provide a 24 hour / 7 day week watch keeping capability. Its role is described at Appendix 1 to Annex A.

c. **Top Level Budget Holders**. Responsibility for the implementation and risk management of security policy and standards has now been formally delegated to TLB Holders, by means of a single letter of delegation from PUS dated 17 August 2001. An extract from this document is at Annex B. Each TLB Holder is required to nominate a Security Risk Manager to advise the TLB on the balance between business needs and security requirements, taking account of affordability, and act as a TLB point of contact with the DSO. A list of the Security Risk Managers in the TLBs is at Annex C: this includes the representatives from MOD Trading Funds. They will form the membership of a new DSO advisory group, the DSO's Risk Managers Forum (DRMF). TLB Holders/TFCEs will be responsible for maintaining an audit trail of their risk management decisions, and for making a formal annual report to the DSO on the state of security in their TLB/TF.

d. **Principal Security Advisers**. The former Sector Security Authorities were abolished on 1 April 2001. In their place, TLB Holders and TFCEs are to appoint their own Principal Security Adviser (PSyA). The services of another TLB may be chosen to provide the relevant security advice but the responsibility and accountability for the application and maintenance of security in their area is vested in the TLB Holder/TFCE. The responsibilities of PSyAs are set out at Annex D. A list of PSyAs is at Annex E.

e. **Defence Security Standards Organisation**. A new organisation – the Defence Security Standards Organisation (DSSO) was established under the DSO on 1 April 2001 to provide an independent security audit capability and a central source of advice on security implementation issues. Its work will in future be integrated into the work of the Defence Audit Committee to meet the requirements of corporate governance. The DSSO will include a central

accreditation function for networked IT systems that cross TLB/Trading Fund boundaries. The responsibilities of the DSSO are set out at Annex F.

JSP 440

7. One of the recommendations of the SSR was that the MOD Security Manual, JSP 440, should be reviewed and rewritten to set out the essential requirements of security in the Department. It should show clearly which standards are mandated and which are appropriate for risk management. The new JSP 440 is unlikely to be produced before 2003; in the meantime, Volumes 1-3 of Issue 2 of the current JSP 440 will be published shortly to incorporate pre-SSR amendments and this note on security responsibilities. Further interim guidance on security policy will be issued in the form of a series of DSO Guidance Notes.

Gloria Craig

Gloria Craig
DSO
SY 326 80462MB

List of Annexes and Appendices

Intentionally Blank

Annex A to DSO Guidance Note No 1

Role and Responsibilities of the Directorate of Defence Security

Role

1. The Directorate of Defence Security (DDefSy) is responsible to the DSO for the formulation and promulgation of security policy for the protection of all MOD information, assets and personnel, including international security arrangements for the sharing of MOD information with other governments and with Defence industry.

Responsibilities

2. DDefSy has the following principal responsibilities:

a. Contributing to the formulation of Government protective security policy and representing the MOD in interdepartmental and international discussions on protective security policy.

b. Formulating and promulgating defence security policy, setting MOD security objectives and providing guidance on their implementation and resource implications.

c. Primary responsibility for nuclear security matters (but on key issues will act only in concert with the Director of Nuclear Policy).

d. Co-ordinating and providing advice to ministers, PUS and CDS on the political and presentational and legal aspects of protective security policy and security intelligence operations.

e. Liaison with the Cabinet Office, Security Service, OGDs and the Civil Police on security policy issues.

f. Developing security policy and providing security advice to companies holding MOD protectively marked assets or information.

g. Advising DCDS(C) on defensive measures to counter the terrorist and extremist threats to MOD personnel and assets in Great Britain and, in consultation with the Counter Extremist Advisory Group (CEAG), setting the counter-extremist alert state for MOD establishments throughout Great Britain.

h. Timely dissemination of security threat information relating to terrorist threats in Great Britain and overseas.

i. Timely dissemination through the JSyCC of electronic threat information relating to the Department's information systems, covering both IT incidents and

electronic attack. The detailed responsibilities of the JSyCC are given at Appendix 1.

j. Oversight of the reporting and investigation of security incidents, and leaks of official information, by TLB Holders/TFCEs, with particular emphasis on the possible need to revise current security policy, and other remedial action.

k. Serving as departmental focus for the application of UK policy for sensitive document handling and dissemination, and representing MOD on the STRAP management board.

l. Enabling Risk Owners to establish the correct balance of risk to Information Systems by advising on security policy and the residual risk.

m. Advice to MOD and to UK Defence Manufacturers on all technical security matters relating to the overseas release of military information; clearance of UK protectively marked equipment and information at UK and overseas defence exhibitions; and for review of Patent Applications and inventions notified by the general public.

n. Support the DSO in identifying the MOD's security education and training needs and in contributing to the formulation of the policy to meet those needs. (Note. This reflects a responsibility placed on the DSO in the Manual of Protective Security. Exercise of this responsibility will have to take account of the Defence Training Review).

o. Preparation of the annual DSO's Report to the DAC, including tasking and collation of TLB Holder/TFCE reports and staffing of follow-up action required.

Accountability

3. DDefSy is accountable through DGS&S to:

a. DCDS(C) and thence to VCDS for the policy on the protection of MOD personnel and assets against terrorists and other extremists including the counter extremist Alert State.

b. The Personnel Director and thence to 2nd PUS for all other aspects of protective security policy.

Appendix 1 to
Annex A to DSO Guidance Note No 1

Role and Responsibilities of the Joint Security Co-ordination Centre (JSyCC)

Role of JSyCC

To act as focal point for information security intelligence, maintain a central source of vulnerability and threat information, and promulgate summaries, alerts and rectification directives as necessary.

Specific Responsibilities

The specific responsibilities of the JSyCC include:

a. Collating progress reports against Threat Change Notices (TCN) and Vulnerability Rectification Directives (VRD).

b. Receiving and collating incident detection information, liaison with the Unified Incident Reporting and Alert Scheme (UNIRAS) and the Federation of Incident Response and Security Teams (FIRST) for all IT related incidents, and determining the nature of response required.

c. Arranging for, and supervising, any necessary external response where inappropriate to be carried out at unit level.

d. Carrying out any necessary post incident analysis.

e. Supervision of the overall information verification program including provision of generic software toolkits.

f. Maintaining a central register of the Minimum Essential Defence Information Infrastructure (MEDII) element of the Critical National Infrastructure (CNI).

g. Direct control of the verification activities associated with MEDII.

h. Provision of MOD contribution to the National Infrastructure Security Co-ordination Centre's (NISCC) virtual organisation, and related aspects of the CNI protection programme.

i. Provision of awareness and training relating to CIS threats, vulnerabilities, and incident handling.

j. Liaison with similar organisations in UK Government, industry, allies, hardware manufacturers, software providers and the police.

Intentionally Blank

Annex B to DSO Guidance Note No 1

Security Delegations to TLB Holders

Extract from PUS's Covering Letter

I look to you to ensure that Departmental security policy and standards set out in JSP 440 are implemented across your TLB. Your Principal Security Adviser (to be appointed by you) will support you and should be consulted whenever you are unclear about specific delegations or need more general advice. Should you or your Principal Security Adviser be unsure about the interpretation and exercise of the delegations or need specialist advice, you should consult the Departmental Security Officer.

Specific Authority

Authority for the implementation of Departmental security policy and standards (set out in JSP 440 and other policy guidance) in your TLB.

Authority to take necessary timely action on receipt of terrorist and other security threat alerts, and when necessary, the co-ordination of BIKINI Alert State and other counter-measures for all units/establishments in your TLB area.

Authority to exempt units/establishments in your TLB area from compliance with armed guarding and other prescribed security measures, within the limits for variation set out in JSP 440 and other MOD policy guidance.

Authority for accrediting IT systems that are delegated to you by the Departmental Security Officer (DSO).

Authority to undertake a programme of assurance activities to verify internal security control processes. This will be subject to audit by the Defence Security Standards Organisation (DSSO).

Responsibilities

You should ensure that your decisions on security adhere to Departmental risk management guidelines.

You should, in consultation with the DSO, appoint a Principal Security Adviser (PSyA) who will be your source of authoritative day-to-day advice. The PSyA should meet minimum core competencies and have received the appropriate training. The PSyA may be appointed from your TLB, or be provided from another, under agreed arrangements. He or she should consult the DSO for specialist advice when needed, including on any cross-TLB issues.

You should nominate a ‘risk manager’ to advise you on the balance between your business needs and the security requirements, taking account of affordability, and to act as the point of contact for the TLB with the DSO.

You should invest in the necessary training and education to ensure that all staff in your TLB are adequately trained and have the right level of security awareness.

You must agree an audit programme for your TLB with the DSO.

You must submit an annual report to the DSO on the state of security in your TLB.

Annex C to DSO Guidance Note No 1

List of Security Risk Managers

TLBs

CINCFLEET - COS(Ops)	R Adm R P Stevens
2SL/CNH - COS 2SL/CNH	R Adm R G Lockwood
CINCLAND - COS LAND	Maj Gen F R Viggers
GOCNI - COS HQNI	Brig A D Leakey
AG - COS AG	Brig K H Cima
CINCSTC - D/CINCSTC	AM G E Stirrup
PTC - COS PTC	AVM R V Morris
PJHQ - CJFORT	AVM P V Harris
CDL - DG Ops	R Adm M G Wood
CDP - XD1	Mr I Fauset
Centre - DGCB	Mr C T Sandars

Trading Funds

DSTL…….. Mr S Mepham
Met Office……... Mr M Sands
UK Hydrographic Office…… Mr S Parnell
DARA……. Capt P R Bishop RN

Intentionally Blank

Annex D to DSO Guidance Note No. 1

Role and Responsibilities of Principal Security Advisers

1. To provide corporate security advice to the Management Board of the TLB Holder/Trading Fund. Oversight and direction of security across the TLB/Trading Fund.

Specific Responsibilities

2. The following are specific PSyA responsibilities:

a. Advice to the TLB Holder/Chief Executive and the Management Board on all security issues that have a corporate bearing on TLB/ Trading Fund business. This includes advice on:

- Interpretation of Departmental Security Policy.
- Evaluation of security risk applicable to the TLB/Trading Fund.
- Implementation measures.

b. Strategic oversight of security activity across the TLB/Trading Fund, ensuring compliance with policy as implemented within the context of risk-based security management.

c. Representing the TLB/Trading Fund corporate interests in all security activity within the department, consulting with business units and agencies as appropriate.

d. Providing the TLB/Trading Fund focal point for the Departmental Security Officer and the Directorate Defence Security.

e. Liaison with other Principal Security Advisers and co-ordinate the sharing of security support activities.

f. Liaison with police, and other security agencies in government and industry as necessary.

g. Ensuring procedures for reporting and investigating security incidents are followed, where necessary conducting investigations.

h. Ensuring security surveys and periodic inspections are carried out in all subordinated establishments.

i. Undertaking a range of tasks associated with those IT systems that are specific to the TLB/Trading Fund, including accreditation, of those IT systems for which the TLB has been delegated responsibility, ensuring compliance with security requirements, and reporting IT security incidents.

j. Development and implementation of revised structures as necessary to meet the full range of TLB Holder's/ Trading Fund Chief Executive's responsibilities that flow from the Security Structures Review.

k. Provision of security guidance to subordinate headquarters, units and establishments across the TLB/Trading Fund as necessary.

l. Development of a security culture within the TLB/Trading Fund that is cost-efficient and makes use of best practice within the context of risk management as applied to business needs.

3. Personnel Security Responsibilities. Post SSR arrangements for the exercise of personnel security responsibilities, including management of risk cases, have still to be finalised. In the meantime the following arrangements will apply:

a. DDefSy is responsible for civilians in the Central TLB, DPA and Trading Funds and their non List X contractors, for List X industry (but TLB Holders are responsible for List X contractors employed at their sites), and for categories such as SCS and MDP managed centrally.

b. The single Services are responsible for their Service personnel wherever they are employed, for civilians employed in Service TLBs (except for categories managed centrally), and for contractors employed at their Service sites.

c. The DLO and PJHQ are responsible for civilians employed in their TLBs (except for categories managed centrally), and for contractors employed at DLO and PJHQ sites.

Annex E to DSO Guidance Note No 1

List of Principal Security Advisers

TLBs

CINCFLEET	Cdre A Du Port 27120PY
2SL/CNH	Cdre A Du Port 27120PY
CINCLAND	Brig R M Brunt (through DACOS G2, Col R White 3394WIL)
AG	Brig R M Brunt
GOCNI	Col D Homer 63397LB
CINCSTC	Air Cdre C R Morgan 7140STC
PTC	Air Cdre C R Morgan 7140STC
PJHQ	Cdre D A Lewis (through SO3/J2X Flt Lt S Wright 46145NW)
CDL	Mr F C Wood 67509EN
CDP	Mr S Macdonald 30620ABW
	Mr P Betts 6765AW+ (wef 04/09/01)
Centre	Mr A Gray 80991MB

Trading Funds

DSTL……..Mr W F Charlesworth, 01980 613424

Met Office…….. Mr J Throssall, 01344 854631

UK Hydrographic Office…… Mr J McCulloch 3363TN

DARA……. Mr F C Wood 67509EN

Intentionally Blank

Annex F to DSO Guidance Note No 1

Role and Responsibilities of the Defence Security Standards Organisation.

1. The DSSO task falls into two main areas:

   a. provision of a centralised IT security accreditation service, acting as a single source for advice and expertise on MOD's increasingly networked IT systems.

   b. provision of an independent security audit capability to enable the DSO to certify that security policy is being implemented adequately and cost-effectively across the whole of MOD and its Trading Funds.

Accreditation

2. DSSO accreditors will advise business managers of the risks to their IT systems and how best to mitigate and reduce them. The decision to accept the residual risk will lie with the business manager in consultation with other stakeholders. If stakeholder interests conflict, resolution will be determined by either DG Info, ACDS (Ops) or CJO in accordance with established crisis response processes.

Security Audit

3. DSSO auditors will focus on assessing the effectiveness of the integrated risk management process of the TLB Holder/Trading Fund Chief Executive (TFCE). The precise methodology will be developed in partnership with TLB Holders/TFCEs in a series of pilot audits that will begin in September 01. Key areas to be addressed include:

- linkage of security risk to corporate objectives,
- common terminology,
- assessment by likelihood and impact,
- dynamic review and reporting,
- effective reaction.

The formal audit process will begin on 01 April 02 and will draw upon the DSO's Annual Report to the DAC to determine the key themes to be examined.

STRAP Administration

4. There are plans for STRAP administration responsibilities currently carried out by Sector STRAP Security Officers (STRAPSOs) to be re-brigaded under the DSSO. Pending implementation of this change, the pre-SSR arrangements are to continue.

Intentionally Blank

DEPARTMENTAL SECURITY OFFICER
GUIDANCE NOTE No 2

Management of Security Risks

Introduction.

1. In common with all other Government Departments, MOD is obliged to adopt a corporate governance process in accordance with HM Treasury Guidance in Dear Accounting Officer (Gen) 13/00. The concept of corporate governance has emerged through the Cadbury Code, the Stock Exchange's 'Combined Code' and the Turnbull Report[1]. In essence, Turnbull Guidelines require companies to *"maintain a sound system of internal control to safeguard shareholders' investment and the company's assets*." This requires organisations to consider the:

- *nature and extent of risk;*
- *acceptable extent and categories of risk; risk appetite;*
- *likelihood and ability to reduce and / or mitigate risk;*
- *cost-benefit of risk controls,*

and "*produce an annual statement of internal control showing how risk is identified, evaluated and managed*." DAO(Gen) 13/00 extended the requirement for such statements to be included in the accounts produced by the public sector with effect from 1 January 2001.

2. In parallel, DCS 17, the SDR and the Security Structures Review (SSR) have recommended changes to the way in which security is managed and controlled in the MOD. The SSR embeds security decision-taking in core management processes at Top Level Budget/ Trading Fund (TLB/TF) level. This note explains how to manage security risk in a way consistent with JSP 503 (Business Continuity) and with JSP 462 (Corporate Governance), which Directorate of Performance & Analysis (D P+A) are producing for the Defence Management Board (DMB). It also examines the link between security risks and the hierarchy of Balanced Scorecard objectives and explains how risk appetite is

[1] The Turnbull Report – Internal Control: Guidance for Directors on the Combined Code

determined. Finally, it outlines the audit process that the Defence Security Standards Organisation (DSSO) will undertake with TLB Holders and Chief Executives of Defence Trading Funds (TFCEs) on behalf of the Departmental Security Officer (DSO), Director General Security & Safety (DGS&S).

Risk.

2. The MOD defines risk generically as ***a future uncertain event that could influence the achievement of departmental objectives and statutory obligations***. The key element is the uncertainty of the outcome; taking a risk may result in benefit or harm. This general definition covers the risk that occurs at all levels and in all areas of departmental activity. Such risk arises from the random nature of events, imperfect or incomplete knowledge, human behaviour, resource and time constraints, and lack or failure of control systems. It is assessed in terms of likelihood and impact using qualitative and quantitative methods and judgement born of corporate and individual experience.

3. Within that generic definition, risk has a more specific meaning in the security context. MOD security policy is laid down in JSP 440 and derives from the Cabinet Office Manual of Protective Security (MPS), revised in April 2000 to incorporate BS 7799 (Information Security Management**). Security risk is perceived as a threat of compromise to the Confidentiality, Integrity and/or Availability of assets** and is defined as *a combination of threat and vulnerability.* The sub-elements of threat and vulnerability are described as the *likelihood of a potentially compromising event taking place* and the *feature or characteristic of an asset that could be exploited in an attack.* Thus, despite the more negative perception of security risk, the consequence is assessed in the same way as generic risk, in terms of likelihood and impact. It is therefore entirely reasonable to make security risk management decisions using the processes and terminology common to the corporate governance mechanisms specified by the DMB for all other departmental risk management. JSP 440 will require some change to reflect this.

Corporate Risk Management.

4. Both D P+A and MPS describe risk management as *a continuous cycle of identifying, assessing, controlling, monitoring, reporting and reviewing risks against objectives identified in a management plan.* BS 7799 also emphasises the need to relate security risks to business harm. The key elements are the dynamic identification and ranking of risks to management plan objectives and the creation of effective control systems to maintain exposure to the likelihood and/or impact at acceptable levels. The generic risk management model being developed by D P+A will allow the DMB to consider the overall "at risk" position of MOD in the light of current control mechanisms and to assess whether this could confound the achievement of DCP objectives.

5. Departmental Corporate Governance policy will be reviewed annually by the DMB to ensure its continued application and relevance. The principles are:

a. Risks should be identified and evaluated in the context of their potential impact on the achievement of objectives.

b. Risks should be managed at the level at which staff have authority, responsibility and resources to take action.

c. The identification and evaluation of risk will become an integral part of performance management.

d. All key decisions should be supported by a risk assessment and risk management plan.

e. The risk management policies developed by policy setting bodies should be compatible with Corporate Governance and risk management policy and guidance.

f. Internal audit and other assurance activities will be based on assessments of risk to objectives.

g. The Directorate of Internal audit will continue to provide the Department's principal source of independent internal audit advice, but will draw on other bodies (both internally and externally as sources of corporate assurance, as appropriate.

6. In practical terms, risk appetite (the range of risk) and tolerance (the level of risk) can be determined by answering such questions as:

a. What risks will we take in pursuit of Management Plan objectives, and what risks are unacceptable?

b. Can we tolerate the level of each accepted risk, and the aggregate level of risk, in the light of current control mechanisms?

c. Are legal, statutory and baseline control requirements met, and at what impact on output, time and cost?

d. What opportunities are lost because of risk aversion?

e. What impact does our risk have on internal and external stakeholders?

f. Where should risk be reduced or increased?

g. Where should regulation/policy be challenged/changed?

There is an evident corollary between this generic approach and a more specific application in regard to security.

Security Risk Management

7. Although functional areas such as security afford scope for a more bespoke approach to identifying risks, security risk should be managed through corporate governance mechanisms. Equally, while the DSO will indicate any specific legal,

statutory or regulatory security baseline objectives, the DMB will determine departmental risk appetite and tolerance through the DCP. But specialist staff input will be required to identify threats accurately, advise on cost-effective risk mitigation (reduced likelihood) and reduction (reduced impact) strategies and indicate whether the residual risk is consistent with any mandated baseline control or legal obligation. The TLB/TF security risk manager will adjudicate in conflicts between business and security interests by considering issues of residual or reasonably foreseeable risk (in the light of existing or proposed controls), practicality and cost. He or she may draw on the DSSO for impartial expert advice. Higher levels of appeal would involve the TLB Holder/TFCE and DSO personally.

The Process

8. Risk management should be implemented as a continuous and auditable process. There is no one mechanism for this, but MOD has accepted a four-stage process - identification, analysis, planning, and control – as best practice. This is illustrated at Annex A. Further guidance is available on the DP+A website on MODWeb.

9. The techniques appropriate to the stages of the risk management process will be familiar to Principal Security Officers (PSyAs); an approach to the process, for example, is described in Supplement 2 of MPS. This Guidance Note does not describe the techniques in detail but simply notes some key considerations:

a. **Risk Identification**. All security risks to business/operational objectives are to be listed. These will be drawn mainly from threat assessments but may include opportunity risks. Risks should be examined from the perspective of all internal and external stakeholders. Consequential risks that arise from the mitigation of primary risks or the granting of waivers/exceptions should be identified. Risks should be grouped against business/operational objectives and by balanced scorecard (BSC) categories. See Annex B.

b**. Risk Analysis.** Risks are to be prioritised in terms of likelihood and impact, and related to the key balanced scorecard risks (between 10-15) identified by the management board. This will make security risk analysis consistent with the

required output, risk appetite, tolerance and mandatory controls. Both qualitative and quantitative methods should be used. The present system of grading threat levels between VERY HIGH (Grade 1) and NEGLIGIBLE (Grade 6) is consistent with D P+A Level 2 methodology, and the Cabinet Office / SSG definitions regarding frequency may also be useful. See Annex C.

c. **Risk Planning**. The key to effective planning is to complete the Risk Register for managing each significant risk. Typically this will include identifying who is responsible for control implementation, the resources to be used, the budget allocation, timescale and mechanism for monitoring and reviewing compliance with the risk management plan. See Annex D. MOD adopts four strategies to respond to risk: Transfer, Tolerate, Treat and Terminate. In many areas it is unlikely that, as provider of last resort, the Department can completely transfer or terminate risk.

d. **Risk Control**. This term covers the processes whereby the effect of planned activity is monitored, reported and reviewed. There is a wide range of control mechanisms, and it is inappropriate to direct which should be used as their utility differs in differing areas. But, in an integrated risk management system, it is essential to use a common methodology to assess their effectiveness. The DMB has adopted a four-category control rating classification (Red, Amber, Yellow and Green) that is wholly applicable to security**:**

Table 1. DMB Risk Control Ratings

Control Rating	Definition
HIGH (Red)	Very serious weakness with significant scope for improving management response (control strategy)
MEDIUM – HIGH (Amber)	Serious weakness with moderate scope for improving management response
MEDIUM (Yellow)	Minor weakness with minimal scope for improving management response
LOW (Green)	Cost-effective and efficient control

In assessing the overall quality of controls, you should consider both the effectiveness of the mitigation/reduction and the efficiency of the control procedure in terms of output, cost and time. You should also consider developing Key Risk Indicators (KRI) to complement other Management Plan Performance Indicators (PI). **Control rating assessments will be required in TLB Holder/TFCE annual reports,** on which the DSO will draw so as to report to the Defence Audit Committee (DAC) and provide the annual Certificate of Assurance (CoA) that will form part of PUS's Statement of Internal Control.

Auditing the Process

10. The CoA cannot rely solely on self-reporting. The DSO will therefore audit TLB Holder's/TFCE's security risk management process. Audit frequency will be conditioned by the criticality of TLB/TF output to DCP objectives, the level of risk in the TLB/TF, and MPS/JSP 440. Alternatively, of course, they will be carried out at the request of the TLB Holder/ TFCE. The audit will help establish how effectively TLB Holders/ TFCEs are discharging the specific security responsibilities delegated to them.

11. Audits will be undertaken by the Defence Security Standards Organisation (DSSO). They will be conducted at the strategic level and will focus on the process for identifying, evaluating, limiting and controlling significant risks. An illustrative example of areas covered is at Annex E.

Gloria Craig

Gloria Craig
DSO
SY 326 80462MB

List of Annexes:

A. Illustration of the Risk Management Process.

B. Exemplar Risk / MP Objective Identification Matrix.

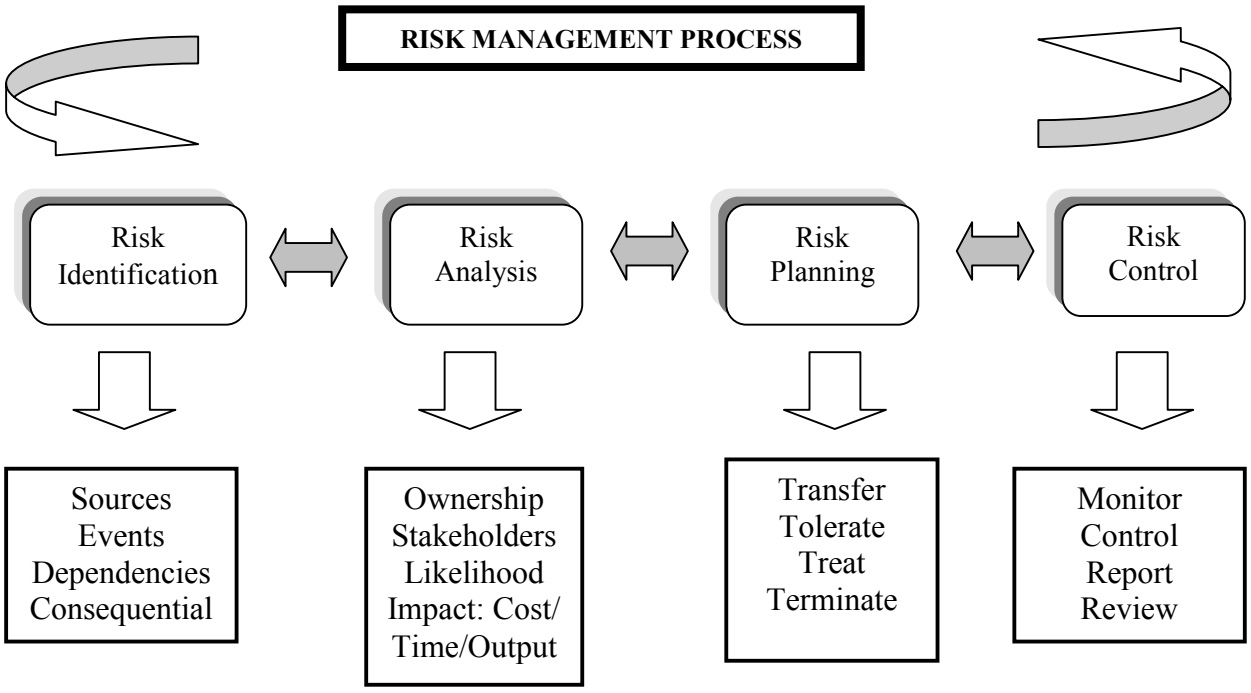
C. Corporate Impact, Threat Level, and Frequency definitions.

D. Exemplar Risk Register.

E. DSSO Audit

Annex A to DSO Guidance Note 2

Illustration of the Risk Management Process

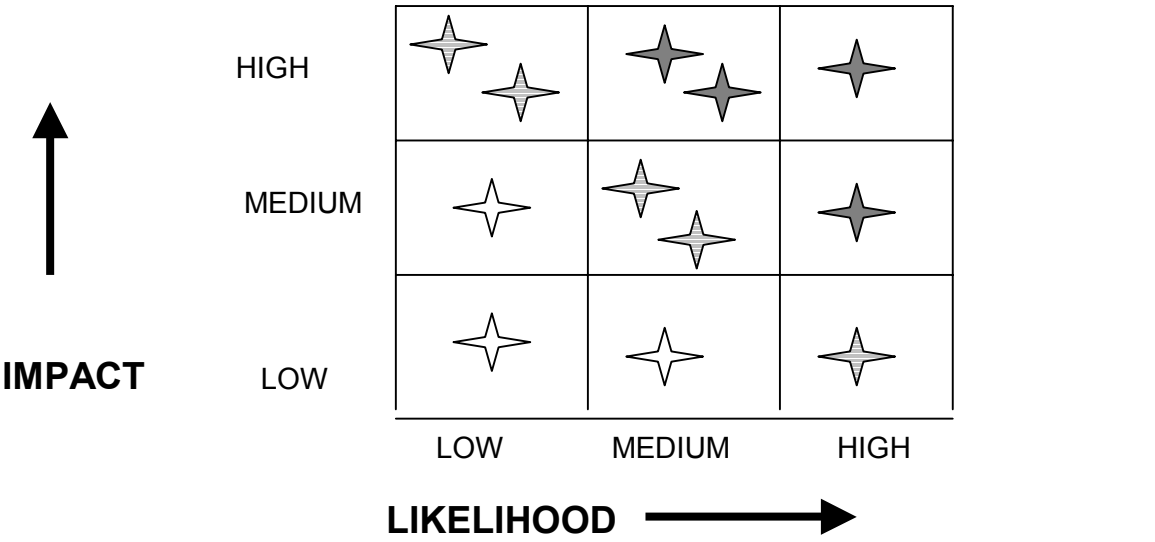


Intentionally Blank

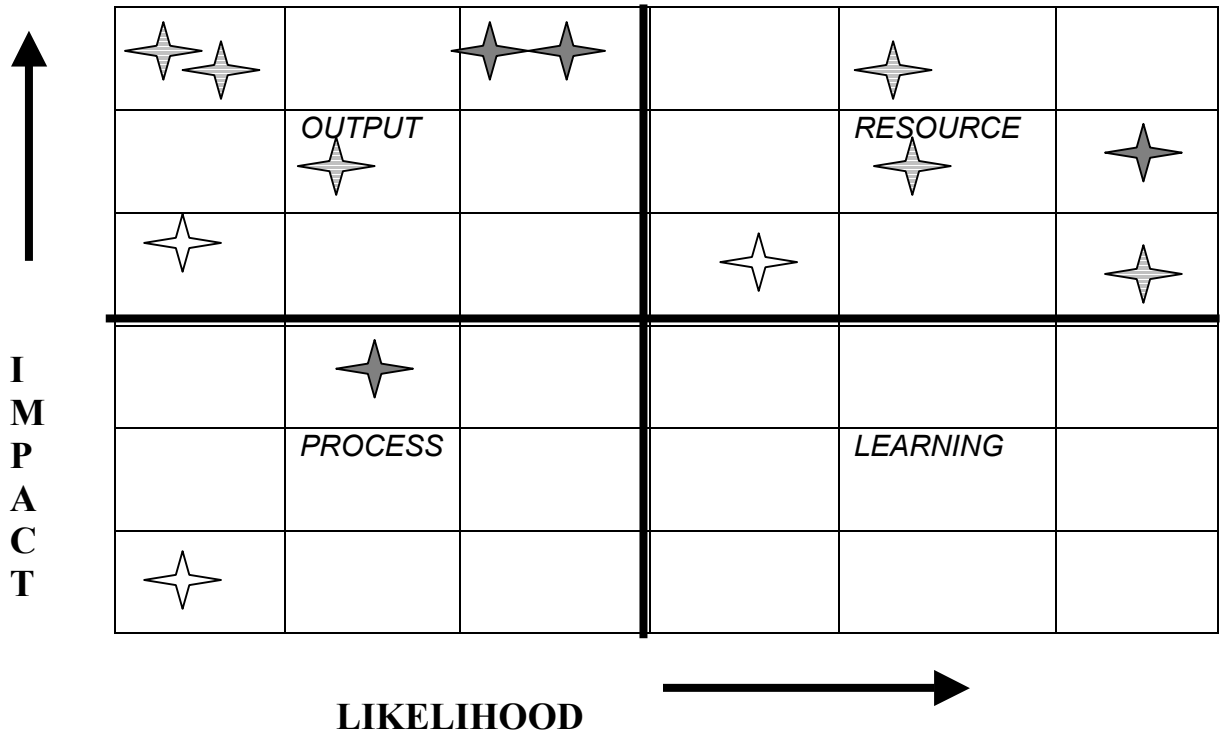
Annex B to DSO Guidance Note 2

EXEMPLAR RISK / MP OBJECTIVE IDENTIFICATION MATRIX

1. TLB Risk Matrix of Top Risks



2. Example of How Risks Might Be Transposed to a TLB Balanced Scorecard



Intentionally Blank

Annex C to DSO Guidance Note 2

IMPACT – D P+A CORPORATE DEFINITIONS

RISK IMPACT Level 1	Corporate definition must apply	RISK IMPACT Level 2	Definitions by appropriate MB
HIGH	Either – has the potential to cause a Defence Balanced Scorecard objective to fail. Or – has a large short term or longer-term impact on the delivery of defence output. This risk would be of concern to the DMB.	HIGH	
		MEDIUM to HIGH	
MEDIUM	Either – has the potential to cause a TLB Balanced Scorecard objective to fail. . Or – has a moderate term impact on the delivery of defence output. This risk would be of concern to the TLB Management Board.	MEDIUM	
		MEDIUM to LOW	
LOW	Either – has the potential to materially affect a TLB Balanced Scorecard objective. Or- has a minor short-term impact on the delivery of defence output .	LOW	
		VERY LOW	

FREQUENCY LEVELS – CORPORATE DEFINITIONS

Chance in next Financial Year	Description	Frequency per year
X 10	Will happen often	10
1	Certain to occur	1
1 in 3	Very likely to occur (highly possible)	0.33
1 in 10	Quite likely to occur (possible)	0.1
1 in 100	Unlikely to occur	10^{-2}
1 in 1000	Very unlikely to occur	10^{-3}

Annex D to DSO Guidance Note 2

EXEMPLAR RISK REGISTER

Risk: **Risk Manager:**

Nature and source of the risk	
How likely is this to happen?	
What is the impact of the risk in terms of output, cost and/or time?	
What controls have we applied to mitigate (reduce the *likelihood* of) the risk?	
What controls have we applied to minimise (reduce the *impact* of) the risk?	
What potential controls have we chosen **not to apply** on grounds of time /cost / practicability?	
How much of the risk is controlled by others? Who are they?	
Are any risks, or elements of them, controllable by our senior management? Have we told them about these risks?	
Is any risk beyond their control?	
What is the control rating for this risk?	
DATE OF LAST REVIEW	

Intentionally Blank

Annex E to DSO Guidance Note 2

DSSO AUDIT

1. Properly, much of the detail of the audit process will be developed in partnership with TLB Holders/ TFCEs in the first year of the DSSO's existence (01 Apr 01 – 31 Mar 02). However, certain key principles will condition that work and can be spelled out here.

2. The purpose of a DSSO audit is to provide a level of assurance about the adequacy of management's embedded security risk management process. To do this, DSSO auditors will focus on the processes in place for the TLB/TF Management Board to identify, analyse, plan and control security risk. In so doing, they will have regard for any legal, statutory or regulatory obligations imposed on the TLB/TF but will not be responsible for compliance checking. It is for the TLB Holder/TFCE to determine the inspection regime required in accordance with DSO Guidance Note No 3, *Security Inspection Policy*. The auditors will focus on the mandatory elements of an integrated risk management process;

- Linking risk to corporate objectives (including baseline objectives)
- Common terminology
- Assessment by likelihood and impact
- Dynamic review and reporting
- Effective reaction
- Assessment of control effectiveness according to the 4 tier "traffic light" system.

3. The audit will be conducted on a collaborative basis. Whilst an assessment of the effectiveness of the risk management process will be a result of this activity, the key outcome will be the provision of realistic and timely advice designed to add business value by improving both control and performance.

Intentionally Blank

DEPARTMENTAL SECURITY OFFICER
GUIDANCE NOTE No 3

Security Inspection Policy

Background

1. The MOD security inspection régime, along with the associated categorisation of MOD establishments for security purposes, has been in place for many years. As a result of the Security Structures Review (SSR), ownership of the security risk and responsibility for risk management has passed to TLB Holders and Chief Executives of MOD Trading Funds (TFCEs). The SSR included the recommendation that the security inspection regime be reviewed.

Aim

2. The aim of this Guidance Note is to establish the policy for security inspections post SSR.

Scope

3. The scope of this note is limited to outlining the DSO's standing requirement for information on security compliance, and to the policy guidance needed by TLB Holders/TFCEs to carry out their security inspection responsibilities. Reference will be made to the complementary process of independent audit to be established as a result of the SSR but only to explain the linkage with inspections, and the distinction between the two activities. Details of the future audit policy, and the way in which a Defence Security Standards Organisation (DSSO) audit team will operate, will be promulgated separately

4. This note is concerned with the policy on inspections of security procedures at establishment level. These inspections are to embrace all aspects of protective security and include checks on the implementation of physical security procedures protecting the Communication and Information Systems (CIS) installations and the electronic

information held by the establishment concerned. However, this inspection régime does not include the separate measures to be taken to check the security of the electronic environment in which the CIS operate. The latter are to be promulgated in Issue 2 of JSP 440 Volume 3, Chap 12.

Definitions

5. Loose use of the terms ‘survey’, 'inspection' and ‘audit’ can cause confusion. The following definitions apply:

a. Survey. A detailed, pre-planned security examination carried out by a specialist team to examine, report and make recommendations on the protective security requirements of an establishment.

b. Inspection. A periodic, on-site review of compliance with security orders, regulations and instructions, conducted by a security team tasked by the TLB Holder /TFCE that owns the risk at the establishment concerned.

c. Audit. An independent review by the DSSO of the systems and structures in place to support the TLB Holders’/TFCEs’ security risk management processes.

Assurance Requirements

6. The Manual of Protective Security (MPS) requires the Departmental Security Officer (DSO):

“to provide an appropriate method for assuring that the required levels of protection is being achieved. As part of this process the DSO should provide the Head of the Department, or agency, with an annual Certificate of Assurance. This certificate is designed to provide a formal assurance that the organisation is achieving the required levels of protective security and to highlight areas of specific security concern.”

In the MOD the DSO delivers this assurance by submitting an annual report to the Defence Audit Committee. This report is dependent on the contributions provided by TLB Holders/TFCEs covering the state of all aspects of protective security for their respective areas of responsibility, reported against criteria and other guidance provided by the DSO. In future, the feedback from the independent audit function carried out by the DSSO will be an important contribution to the DSO's report.

7. While management of the security risk, in accordance with the policy guidance in DSO Guidance Note No. 2, will be delegated to TLB Holders/TFCEs, it will be necessary to have consistent sets of baseline criteria to inform not only TLB decisions on resource allocation and the inspection regime, but also the DSSO audit process. The majority of these criteria will be in the form of advisory guidance although a few will be mandatory. These baseline criteria will be promulgated in DSO Guidance Notes pending publication of the New JSP 440. This approach will involve the use of two tools in particular:

a. A common approach to the categorisation of establishments.
b. Common guidance on the inspection régime.

Categorisation of Establishments

8. Categorisation of MOD establishments will maintain a consistent baseline across the Defence spectrum and assist TLB Holders/TFCEs with the risk management process that will inform their resource allocation decisions. It is, therefore, important that TLBs are able to give their establishments a security profile, assessed against common definitions. The adoption of one combined matrix will take account of the full threat spectrum and Risk Impact Level. It will facilitate a comprehensive approach to security inspections to include, where relevant, the personnel, physical and procedural security measures which apply to CIS installations within sites. This combined matrix is shown in outline below:

Table 1- Combined Matrix

Asset Category	Risk Impact Level	Guarding Category		
		P1	P2	P3
A1	High			
A2	Medium High			
B1	Medium			
B2	Medium Low			
C1	Low			
C2	Very Low			

Notes:

1. Categories A1-C2 relate to all aspects of the threat to the security of information and materiel (assets) and are based on new definitions. These definitions are given at Annex A.

2. Categories P1-P3 relate to the threat to life posed by terrorism and retain pre-SSR JSP 440 definitions used to determine guarding criteria. These definitions are also reproduced at Annex A.

9. The process of categorising establishments is to involve an assessment of both the establishment's asset risk impact level and the guarding requirement, producing a combined value, e.g. B2/P1.

10. Individual establishments and lodger units within a large site should be assessed according to their individual assets and vulnerabilities. The fact, for instance, that the perimeter and Service living accommodation on a large site is designated P1 for 'threat to life' reasons and includes a sensitive unit that requires a Category A2 rating, should not be taken to mean that each and every establishment on the site should be accorded the same Category A2 rating regardless of the activities conducted within its own discrete area. Where there is a specific area within an establishment that requires a higher category, e.g. an operations or communications centre, it may be categorised separately from the remainder of the establishment and the remainder may then be placed in a lower category for inspection purposes.

Categorisation of Communications and Information Systems

11. There are four Criticality Levels (CL1, CL2, CL3 and CL4), which are used to gauge the impact of any disruption to CIS, or exploitation of any information they contain. The criteria for establishing the right criticality level for CIS are in Issue 2 of JSP 440, Volume 3 Chapter 1.

Security Survey and Inspection Regimes

12. TLB Holders/TFCEs will be required to carry out a security survey when an establishment is first formed, is reorganised and changes its role, or on completion of major works services. The comprehensive survey report will be the baseline against which future protective security of the establishment will be measured. Additional security surveys may be conducted in response to special requirements of the TLB Holders/TFCEs. This is no change to the pre-SSR regime.

13. The pre-SSR inspection régime was mandatory in character, and a new régime is required to reflect TLB Holders'/TFCEs' delegated responsibilities for security risk management and a more flexible approach to managing all aspects of the changing threat. Threats to Defence establishments vary widely, as do their vulnerabilities. Although every establishment should be subject to periodic formal security inspection, the programme should reflect these differences. In determining the frequency of inspections for establishments within their area, TLB Holders/TFCEs will need to consider various factors. These will include: the criticality of the establishment's output in meeting management plan objectives, the risk profile, the outcome of previous inspections and audits, turnover of key personnel, and any mandated requirements. TLB/TF inspection reports will provide a major input into the DSO's annual Certificate of Assurance. TLB Holders/TFCEs may elect to supplement formal inspections by advisory visits and by the completion of security questionnaires. The guideline for the periodicity of inspections is shown in the categorization matrix below:

Table 2 – Inspection Periodicity Matrix

Asset Category	Risk Impact Level	Inspection Periodicity (years)	Guarding Category		
			P1	P2	P3
			Inspection Periodicity (yrs)		
A1	High	1	3	4	6
A2	Medium High	2	3	4	6
B1	Medium	3	3	4	6
B2	Medium Low	4	3	4	6
C1	Low	5	3	4	6
C2	Very Low	6	3	4	6

14. It will be for TLB Holders/TFCEs to determine the detailed form of their own inspections, adjusting the emphasis to take account of the importance of the establishment's outputs to the TLB/TF, its risk profile and security history. Guidance on best practice on the form and conduct of security inspections will be promulgated separately.

15. TLB Holders/TFCEs may opt to inspect at more frequent intervals than given in the above matrix, in accordance with their risk management and resource decisions. If they elect to inspect establishments in a given category at intervals greater than the periodicity indicated in the matrix, TLB Holders/TFCEs will be required to provide an audit trail and rationale for the decision as part of the process of their reporting of security assurance and subsequent audit.

16. For many establishments, the guidance periodicity for asset and guarding categories will differ. It will be for TLB Holders/TFCEs to schedule their inspections programme so that both asset and guarding elements are inspected satisfactorily. As a guide, when asset and guarding category periodicities differ, the asset category periodicity should be taken as the driver for the conduct of comprehensive inspections, and the guarding category periodicity for supplementary inspections of relevant Counter Terrorist (CT) measures. TLB Holders/TFCEs might, for example, choose to schedule these additional CT inspections around the mid point between comprehensive inspections. The following examples illustrate the options open to TLB Holders / TFCEs:

a. An establishment is categorised B1/P2, giving a periodicity for inspections of 3 and 4 years. A TLB Holder might choose to merge the two categories and carry out a comprehensive inspection (including a CT inspection) between the 3 and 4 year points Alternatively, the TLB Holder might choose to conduct all aspects of security inspection at the 3 year point, and carry out a supplementary CT-orientated inspection at the 4 year point.

b. An establishment is categorised C2/P2, giving periodicity for inspections of 6 and 4 years. The TLB Holder might choose to adhere to the guideline periodicity, or to advance the CT inspection to the 3 year mid-point between comprehensive inspections.

Conclusion

17. Following the SSR, the implementation of protective security in the MOD is the responsibility of TLB Holders / TFCEs as owners of the risk. They will have support from specialist security staffs. TLB Holders/TFCEs will need to prioritise the allocation of inspection resources in accordance with their interpretation of a Defence-wide system of categorising establishments dependent on the threat faced. The implementation of protective security by TLB Holders/TFCEs may involve variation from advisory baseline criteria set by DDefSy in accordance with their risk management decisions, and they will maintain an auditable record of their security decisions and processes.

Gloria Craig

Gloria Craig
DSO
SY 326 80462MB

Annex:

A. Definitions for the Categorisation of Establishments.

Intentionally Blank

Annex A to DSO Guidance Note No 3

Definitions for the Categorisation of Establishments

1. The combined matrix to be used in determining the risk profile of an establishment is produced by bringing together separate assessments on all aspects of the threats to information and material (assets), and on the threat to life posed by terrorism. The former involves selection of a category in the range A1-C2, the latter a category in the range P1-P3. In each case the categories selected are consistent with the Level 2 matrix of Risk Impact Levels that are referred to in the Risk Management Guidance at Annex C in DSO Guidance Note No. 2.

2. The definitions to be used in determining the categorisation of an establishment in relation to the threats to information and material (assets) are as follows:

Category A1. (Risk Impact High). Establishments with a nuclear role and holding nuclear weapons or Special Nuclear Material (SNM).

Category A2. (Risk Impact Medium High). Establishments holding assets or carrying out an exceptionally sensitive or critical role, the loss, disruption or compromise of which would cause *exceptionally grave damage* to the operational effectiveness or key business output of the TLB/TF or MOD.

For example: Establishments, including branches of HQs, with an exceptionally sensitive or critical role; or whose main outputs depend upon processing information on a CL1 CIS system; or carrying out TOP SECRET research and development activity of major importance to UK defence capability.

Category B1. (Risk Impact Medium). Establishments holding assets or carrying out a very sensitive or critical role the loss, disruption or compromise of which would cause *serious damage* to the operational effectiveness or key business output of the TLB/TF or MOD.

For example: Establishments, including branches of HQs, with a very sensitive or critical role whose key outputs depend upon processing information on a CL2 CIS system; or carrying out SECRET research and development activity.

Category B2. (Risk Impact Medium Low). Establishments holding assets or carrying out a role the loss, disruption or compromise of which would cause *damage* to the operational effectiveness or key business output of the TLB/TF or MOD.

For example: Establishments, including branches of HQs, with a sensitive or critical role; or with a deployable operational role in a readiness cycle or having an essential force generation function; or whose key outputs depend upon processing information on a CL3 CIS system.

Category C1. (Risk Impact Low). Establishments holding assets or carrying out a role the loss, disruption or compromise of which would cause *difficulty* in maintaining the operational effectiveness or a key business output of the TLB/TF or MOD.

For example: Establishments, including branches of HQs and units not included in Category A or B holding protectively marked information or equipment mainly at CONFIDENTIAL level or below with CL4 CIS systems that are not critical to key TLB/TF business or operational outputs.

Category C2. (Risk Impact Very Low). Establishments holding assets or carrying out a role the loss, disruption or compromise of which would cause *negligible damage* and would not significantly degrade the operational effectiveness or a key business output of the TLB/TF or MOD.

For example: Establishments, including branches of HQs and units not in Category A or B that do not hold protectively marked information or equipment above RESTRICTED level or full bore weapons.

3. The definitions to be used in determining the categorisation of establishments in relation to the terrorist threat are those agreed and in Issue 2 of JSP 440, Vol. 1, Chap 5. Details are as follows:

a. **Category P1** Buildings and areas (excluding Service Families Accommodation (SFA) areas) in which identifiable and/or uniformed Service personnel live overnight on a regular basis, or are permanently occupied for work, e.g. barracks, communication sites manned over 24 hours. These establishments must, at all times, be protected by a guard force capable of being armed. If armed guarding has been ordered, an armed guard is to be posted at each active entrance/exit and an armed Quick Response Force (QRF) must be permanently available. Armed personnel guarding gates may be included in the QRF provided their gates can be closed and secured for the duration of the alert. At least one gate will need to remain in operation for possible access of emergency services.

b. **Category P2**. The following buildings and areas:

(1) Those in which identifiable and/or uniformed Service personnel work on a regular basis, e.g. during normal, weekday working hours, frequently in conjunction with MOD civilian employees.

(2) Those where weapons, ammunition and explosives considered to be Attractive to Criminals and Terrorist Organisations (ACTO) are stored.

These establishments must at all times be covered by a QRF capable of being armed. QRFs found from MOD sources must be armed if armed guarding has been ordered. If the QRF is found from HDPF, decisions on arming will rest with the police chain of command. Permanent static armed guards at entrances and exits are not required.

c. **Category P3**. Other buildings and areas:

(1) Those in which people live and work on a part-time, irregular basis, e.g. certain training camps. Some training camps are used so extensively that they need to be treated as if they were regularly occupied.

(2) SFA areas, and buildings and areas outside the scope of P1 and P2 that are recognised MOD/Service social centres, e.g. NAAFI clubs, recreation clubs or Messes in which people are not accommodated.

(3) Wholly or predominantly civilian manned Defence establishments. Service personnel employed at these sites should wear civilian clothing, unless their function demands that uniform be worn. TLB/TF Security Staffs will then advise whether the establishment should be categorised as P2.

Armed guards and QRFs will not normally be deployed at these establishments, except at BIKINI alert states AMBER or RED. Heads of Establishment (HOE) are to make appropriate contingency plans for periods of increased alert state.

DEPARTMENTAL SECURITY OFFICER
GUIDANCE NOTE No 4

Defence ID Cards and the Introduction of Generic Passes

Background

1. The reorganisation of the Department's security structures following the Security Structures Review (SSR) provides an opportunity to rationalise the pass system across the MOD, thereby increasing efficiency and reducing costs, while at the same time retaining current security levels. Under the post SSR security structure that took effect on 1 April 2001, responsibility for implementation of security is clearly vested in Top Level Budget Holders/Commanders in Chief and Chief Executives of MOD Trading Funds (TLB/Comd/TF). There will, however, be a continuing requirement for guidance on base-line standards and common criteria, to ensure consistency of security compliance across the Department, particularly where information or other assets are being shared or passed from one TLB/Comd/TF to another.

2. The policy on ID Cards and Passes is one such area where co-ordination by the Centre is required if access to units/establishments across the Department is to be efficiently and securely managed. It is stressed, however, that nothing in any policy shall interfere with the Head of Establishment's/Commanding Officer's (HoE/CO) ultimate responsibility for the security of his/her establishment and, therefore, he/she will have the final say on authorising entry to that particular site.

Strategic Policy

3. The MOD policy on Identity Cards and Passes issued by the Director of Defence Security (D Def Sy) is intended to provide a framework upon which individual TLB/Comd/TF can develop consistent implementation of their access control régimes. The strategic intent, developed in response to the direction given by 2nd PUS, is that MOD employees, both Service and civilian, should be able to move about the MOD estate with the minimum amount of security checks commensurate with the prevailing threat levels. Annex A is a wiring diagram of the security structure within MOD as it applies to this issue.

4. The key areas of central policy are as follows:

a. Defence ID Cards are to be accepted as a means of identification and a pass at all MOD establishments (other than *Special Areas*), at which the holder has legitimate business.

b. Generic MOD Passes will be gradually introduced across the Department as agreed by TLB/Comd/TF in consultation with D Def Sy through the Defence Identity Card and Access Control Working Group (DIDCAC).

General Principles

5. The policy has additionally been guided by the following principles:

a. The HoE/CO is responsible for the security of his/her establishment and, therefore, has the right to control entry.

b. MOD employees should be required to carry as few passes as are absolutely necessary and there is to be a standard acceptance policy for ID cards and passes across the MOD.

c. No policy or guidance issued should preclude the requirement for additional passes to allow access to sensitive or hazardous sites or areas within establishments. However, such a requirement is to be fully justified, clearly defined by the HoE/CO and agreed by the TLB/Comd/TF Principal Security Advisor (PSyA). In other words, personnel should not be required to hand over or show one pass or ID card simply to be issued with another one.

d. The generic new pass designs, which have been approved by the PSyAs, shall be gradually introduced across the MOD, within a timescale agreed between D Def Sy and the appropriate PSyA. However, those local designs currently in use should run their course in order to avoid waste. Additionally, those establishments whose staff have no requirement to visit any other MOD establishment(s) may continue to use locally produced single site passes.

e. D Def Sy will grant authority to organisations to allow them to produce approved ID cards and passes and publish appropriate contact numbers to allow security personnel to verify the authenticity of cardholders.

f. No change is required to current arrangements made by PJHQ for Overseas Commands and joint operations overseas, and by HQ NI, other than the requirement to provide data to the central database.

Further Information

5. The revised policy is set out in the following Annexes:

a. Definitions - Annex B.

b. Defence Identity Cards – Annex C.

c. Generic MOD Establishment Passes - Annex D.

d. Application for new ID Card or Pass Design – Annex E.

e. MOD central database – Annex F.

Effective Date

The introduction of the generic MOD Pass, and the acceptance of Defence Identity Cards to provide access across the Defence estate, is to take effect with effect from 1 October 2001. Additionally, the possible introduction of a generic pass for MOD vehicles is currently being discussed with TLB/Comd.

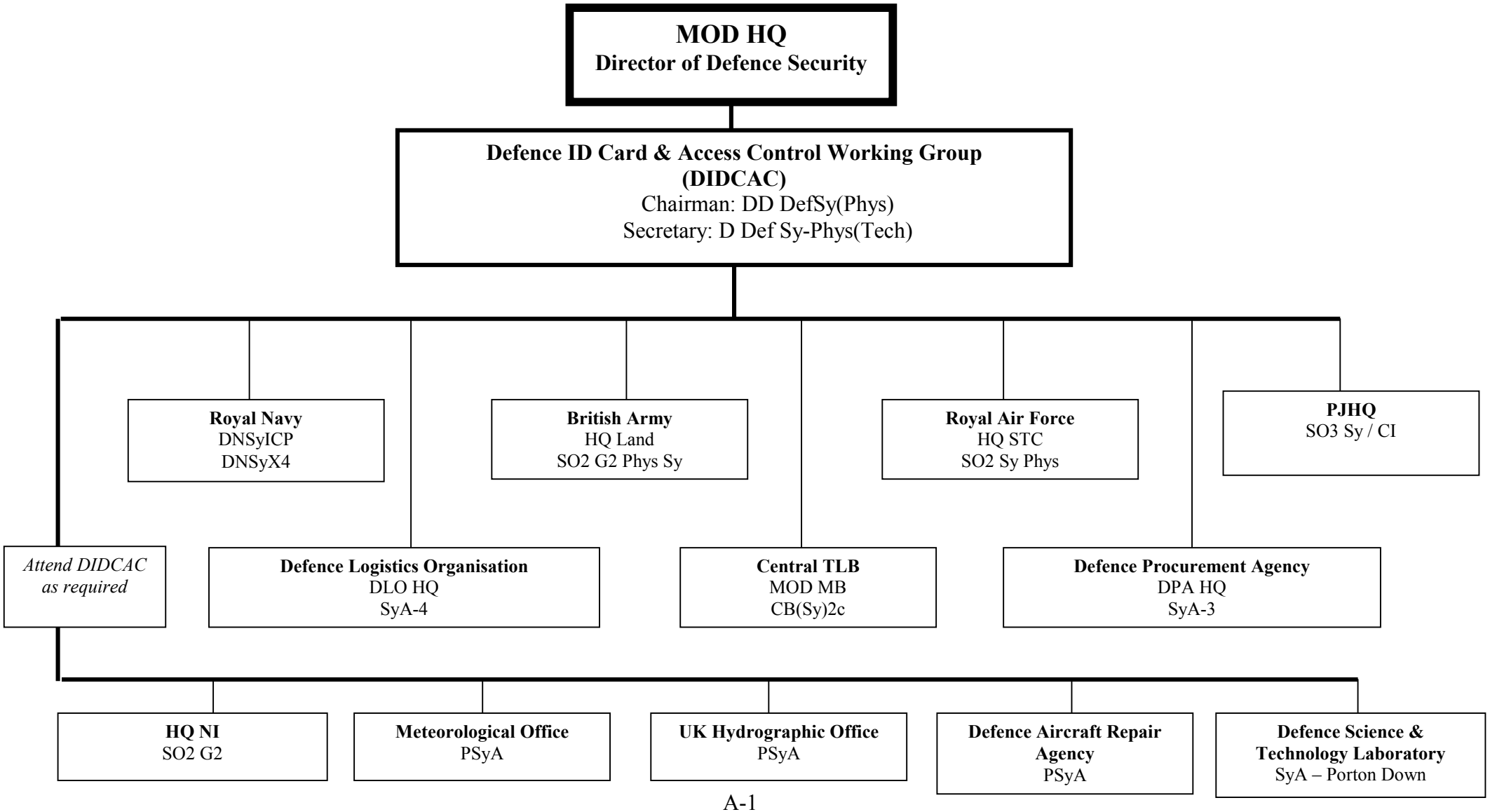
Gloria Craig

Gloria Craig
DSO
SY 326 80462MB

Intentionally Blank

Annex A to DSO Guidance Note No 4

SECURITY RESPONSIBILITIES FOR ID CARDS AND PASSES WITHIN MOD



Intentionally
Blank

Annex B to

DSO Guidance Note No 4

DEFINITIONS

1. The following definitions apply:

a. **MOD Establishment**. In terms of ID Cards and Passes, an Establishment is a controlled area, the access control policy for which is the responsibility of one person (the HoE/CO). Within an establishment there may be any number of HQ formations, independent Service units or MOD business units. These are collectively termed 'lodger' units and are required to comply with the HoE/CO's access control policy.

b. **Controlled Area**. An area which may be entered only upon the presentation of valid appropriate identification.

c. **Special Area**. In terms of ID Cards and Passes a Special Area is one which requires additional control of entry procedures on security or health and safety grounds. This means that a local pass will be issued for entry into such areas and that a Defence ID Card or Generic MOD Pass will not grant automatic access. To define an entire establishment as a Special Area will require the approval of the TLB/Comd/TF PSyA. Sections, sub-units and lodger units within an establishment can be defined as Special Areas by the HoE/CO if required.

d. **Defence Identity Card**. A document (design approved by D Def Sy) issued to a member of HM Forces confirming the identity of the bearer. A Defence Identity Card is authorised for use as a pass. Defence ID cards are administered and produced via the appropriate master personnel database of the employing Service. (A non-compulsory MOD Civil Servant ID Card is being considered and if introduced will be issued to civilian personnel who need to identify themselves within operational theatres, NATO military establishments or to outside agencies. Such cards would become part of the suite of Defence Identity Cards with the same status as those issued to HM Forces).

e. **Generic MOD Pass**. This new document (design approved by D Def Sy) is anonymous as to area, enabling the registered holder to enter a controlled area or number of areas. Such passes may be issued to:

- MOD Civil Servants, and Members of HM Forces if required.
  Colour coded GREEN and of two types (Security Check or Basic Check)

- Personnel from Other Government Departments.
  Colour coded BLUE and of two types (Security Check or Basic Check)

- Contractors.
  Colour coded RED and of two types (Security Check or Basic Check)

- Other personnel as approved by the HoE/CO for access to a single site.
  Colour coded YELLOW and of one type only (Basic Check)

f. **Local Pass**. A document, (design approved by D Def Sy) anonymous as to area, that is issued by establishments who are not yet able, or have no need, to issue Generic MOD

Passes. It may also be document anonymous as to area, enabling the registered holder to enter a single Special Area.

g. **Certificate of Credentials**. A document, (design approved by D Def Sy) which establishes the identity and any official capacity of the holder.

h. **Permit**. A document approved by the HoE/CO or PSyA, issued to authorise the performance of a specific action within the HoE/CO or PSyAs area of responsibility.

i. **Membership card**. An administrative document authorising the bearer to enjoy specified facilities.

g. **TRIGRAM**. A unique three letter identifier on the front of the MOD Generic Pass which is issued by D Def Sy through TLB/Command PSyAs. Its purpose is to identify the establishment or group of establishments to which the pass holder has authorised access as agreed by the appropriate TLBs/Commands.

k. **SP Number**. A unique number issued by D Def Sy through TLB/Command PSyAs to pass production units. It is to be printed on all types of identity documentation, pass or permit (including vehicular), issued by that unit. The number confirms the authority of the facility to produce the appropriate cards and allows D Def Sy to return lost cards to the correct establishment. *(All establishments are to ensure that their cards include an SP number – if not units should apply for one using the form at Annex E).*

Annex C to
DSO Guidance Note No 4

DEFENCE IDENTITY CARDS

1. Defence ID cards will be accepted as passes to all MOD establishments at which the holder has legitimate business. The following cards are currently authorised:

a. **Royal Navy ID Cards**.

- Royal Navy)
- Royal Naval Reserve)
- Royal Fleet Auxiliary) (*Form S1511 Revised 4/98)*
- Royal Navy Exchange)
- Royal Navy Careers Service)
- Royal Navy Retired (Retired Officer Grades) (*Form S1511 8/95)*

b. **British Army ID Card**.

- British Army *(MOD Form 90)*

c. Royal Air Force ID Cards.

- Royal Air Force *(RAF Form 1250)*
- Royal Air Force Reserve *(RAF Form 2185)*
- Royal Air Force Civilian *(RAF Form 7400)*

d. **MOD Civil Servant ID Cards**. *(gradually being introduced)*

2. The wording on the back of all Defence ID cards is to be as follows:

> **"This is an official document. Its unauthorised possession, use, retention, alteration, reproduction, destruction or transfer to another person is an offence.**
>
> **The holder must produce this card if requested to do so by a duly appointed person in the execution of his/her duty. Its loss must be reported to the issuing authority immediately.**
>
> **On entering, leaving or within establishments all persons are liable to search.**
>
> **IF FOUND, THIS PASS SHOULD BE PLACED IN THE NEAREST POST BOX FOR RETURN TO: FREEPOST, PO BOX 3037, LONDON N1 IBR ."**

Single Services/TLBs//TFs who wish to use their own return FREEPOST address for lost ID cards, as in the case of the Royal Navy, should arrange this directly with Consignia (new name for the Post Office) and amend the above wording accordingly.

3. Defence ID Cards are to be produced at central locations appropriate to the employing Service. Their issue is to be carefully controlled and recorded against the holder's service or staff number. All cards are to have a unique watermark® number which is to be recorded in the issuing database.

4. Security staffs who wish to authenticate Defence ID Card should contact the following:

a.	Royal Navy Card	RN/Army ID Card Production Unit. Civil: 02392 702679 VPN: 93844 2679
b.	British Army Card	*As above.*
c.	Royal Air Force Card	HQ RAF P&SS Force Operations Room Civil: 01462 851515 Ext 8218/8219 VPN: 95381 8218/8219
d.	MOD Civil Servant Card	*To be confirmed.*

5. Defence ID cards are to be returned to the issuing/release authority for cancellation when the holder is no longer entitled, under instructions issued by the single Services.

Annex D to
DSO Guidance Note No 4

GENERIC MOD ESTABLISHMENT PASSES

1. D Def Sy has approved a generic design for MOD establishment passes. Each establishment or group of establishments will have a unique three letter 'TRIGRAM' which will indicate the access rights of the holder.

2. There are four types of pass that use the generic design as follows:

a. MOD Employee. Issued to all MOD civilian employees not in possession of a MOD Civil Servant ID Card and may be issued to Service personnel on a temporary basis if required (eg their Service ID card will not work in an establishment's Automated Access Control System (AACS)). This pass will authorise entry into the issuing establishment and may be accepted at other establishments on agreements reached between appropriate PSyAs.

b. Other Government Departments. May be issued at the discretion of the HoE/CO to the following:

- Staff from other UK Government Departments (OGD) requiring regular access to MOD establishments.
- List X company personnel permanently employed at DLO or DPA establishments.
- Personnel from OGD or foreign armed forces seconded to the MOD.

This pass will authorise entry into the issuing establishment and may be accepted at other establishments on agreements reached by the appropriate HoE/CO and approved by their respective PSyAs.

c. Contractors. May be issued at the discretion of the HoE/CO to contractors who need regular access to a MOD establishment. This pass will authorise entry into the issuing establishment and may be accepted at other establishments on agreements reached by the appropriate PSyAs.

d. Single Site Pass. May be issued at the discretion of the HoE/CO to the following:

- Local tradesmen / taxi drivers.
- Civilian members of sports / social clubs.
- Local government or emergency services officials.

This pass will authorise entry only to the issuing establishment.

3. Generic MOD establishment passes will have periods of validity as follows:

a. MOD Employees:

(1) Civil Servants – Maximum 5 years or any shorter period determined by PSyA or HoE/CO.

(2) HM Forces – In post tour length to a maximum of 3 years or any shorter period determined by PSyA or HoE/CO.

b. .Other Government Departments. Maximum 3 years or any shorter period determined by PSyA or HoE/CO.

c. Contractors. For the length of the appropriate contract to a maximum of 3 years or any shorter period determined by PSyA or HoE/CO.

d. Single Site Pass. Maximum 3 years or any shorter period determined by PSyA or HoE/CO.

4. The wording on the back of all generic passes cards is to be as follows:

"This is an official document. Its unauthorised possession, use, retention, alteration, reproduction, destruction or transfer to another person is an offence.

The holder must produce this card if requested to do so by a duly appointed person in the execution of his/her duty. Its loss must be reported to the issuing authority immediately.

On entering, leaving or within establishments all persons are liable to search.

IF FOUND, THIS PASS SHOULD BE PLACED IN THE NEAREST POST BOX FOR RETURN TO: FREEPOST, PO BOX 3037, LONDON N1 IBR ."

Single Services/TLBs/TFs who wish to use their own return FREEPOST address for lost passes, as in the case of the Royal Navy, should arrange this directly with Consignia (new name for the Post Office) and amend the above wording accordingly.

Annex E to
DSO Guidance Note No 4

REQUEST FOR NEW MOD IDENTITY CARD/PASS OR CERTIFICATE OF CREDENTIALS DESIGN

	Unit/Establishment	Appointment Name	Telephone Number
From:			
To:	RN Units: Army Units (excluding NI): RAF Units: PJHQ Units: DLO Establishments: DPA Establishments: Central TLB Establishments: Trading Fund	DNSyICP – DNSy (X4) HQ Land – SO2 G2 Phys Sy HQ STC – SO2 Sy Phys PJHQ – SO2 J2X DLO HQ – SyA-4 DPA HQ – SyA-3 MOD MB – CB(Sy)2c *Appropriate TF PSyA staff*	

Please find enclosed a copy of new pass/ID Card/Certificate of Credentials* design for your approval and the issue of an SP number and/or TRIGRAM.*

Name:
Rank/Grade:
Appointment:

For TLB/Comd/TF PSyA Use:

This design is recommended / not recommended and forwarded to D Def Sy for approval.

Name:
Rank/Grade:
Appointment:
Tel Ext:

For D Def Sy Use:

This pass/ID card/Certificate of Credentials design is approved / not approved for the following reason(s):

The TRIGRAM is: ☐ The 'SP' Number is ☐

D Def Sy-Phys(Tech)
for Director of Defence Security

Intentionally
Blank

Annex F to
DSO Guidance Note No 4

FUTURE MOD CENTRAL PASS DATABASE

1. Ultimately, D Def Sy intend to submit a proposal to have a central database of all passes, ID cards and where appropriate the security clearance levels of personnel. Careful consideration is being given to the associated security and data protection issues and a trial system called Site Access Management Systems Link (SAMSLINK) is currently being evaluated.

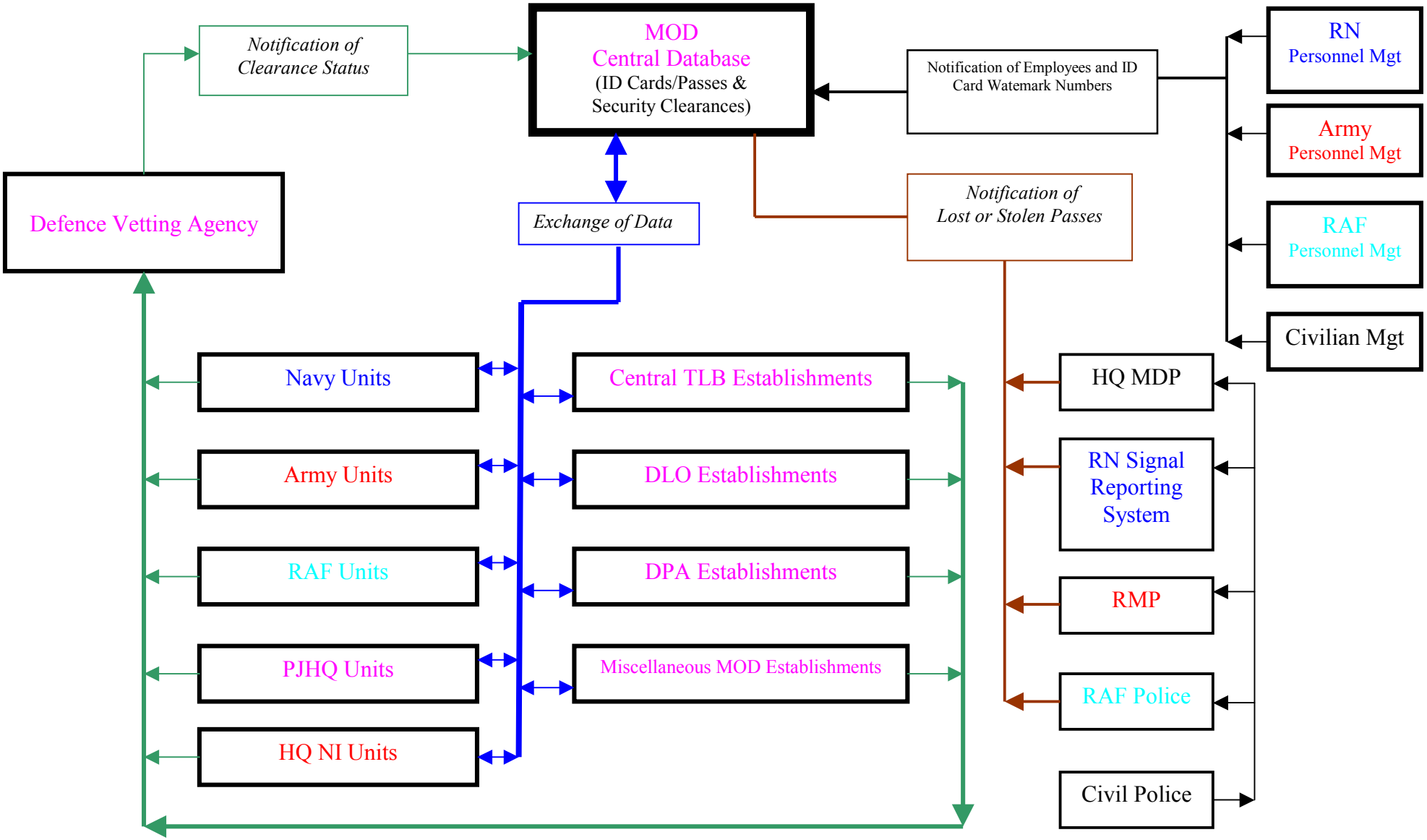
2. Initial indications from the trial suggest that considerable savings can be achieved, in both terms of time and cost, in the secure processing of visitors to MOD establishments and the authentication of valid MOD ID cards and passes. Additionally, the system can be used by establishments for asset tracking, traffic management and for the production of building or site occupancy data in the event of an emergency.

3. Much work and consultation is still required before such a system can be introduced. However, D Def Sy is co-ordinating its efforts with staff from DG Info and their work on smart cards. In the meantime, two initial wiring diagrams of the proposed system are at Appendix 1. Comments regarding SAMSLINK or the proposed central database are invited and are to be addressed to D Def Sy-Phys(Tech) through the appropriate PSyA staff officer detailed in Annex A

Intentionally
Blank

Appendix 1 to Annex F

PAN-MOD SITE ACCESS MANAGEMENT SYSTEM
CENTRAL DATABASE – ID CARDS & PASSES



Intentionally
Blank

MOD SECURITY SITE ACCESS MANAGEMENT UNIT / ESTABLISHMENT DIAGRAM