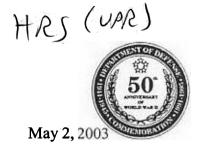HRS (UPR)

DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

May 2, 2003

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
　　　　　　　　　CHAIRMAN OF THE JOINT CHIEFS OF STAFF
　　　　　　　　　UNDER SECRETARIES OF DEFENSE
　　　　　　　　　ASSISTANT SECRETARIES OF DEFENSE
　　　　　　　　　GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
　　　　　　　　　INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
　　　　　　　　　ASSISTANTS TO THE SECRETARY OF DEFENSE
　　　　　　　　　DIRECTORS OF THE DEFENSE AGENCIES
　　　　　　　　　DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Collection, Reporting, and Analysis of Terrorist Threats to DoD Within The
　　　　　United States

　　　　The Secretary of Defense has repeatedly underscored that the nation's war on
terrorism ranks among the Department's highest national security priorities. Much has
been accomplished by DoD's intelligence, counterintelligence, law enforcement, and
security components to counter the terrorist threat in the wake of September 11th, 2001,
however, there is more to be done. While DoD has an established process to identify,
report, and analyze information regarding foreign terrorist threats, we have no formal
mechanism to collect and share non-validated domestic threat information between
intelligence, counterintelligence, law enforcement and force protection entities and
subject that information to careful analysis for indications of foreign terrorist activity.

　　　　A new reporting mechanism, the "TALON" report, has been established to provide
a means to capture non-validated domestic threat information, flow that information to
analysts, and incorporate it into the DoD terrorism threat warning process. A TALON
report consists of raw information reported by concerned citizens and military members
regarding suspicious incidents. Information in TALON reports is non-validated, may or
may not be related to an actual threat, and by its very nature may be fragmented and
incomplete. The purpose of the TALON report is to document and immediately
disseminate potential threat information to DoD personnel, facilities, and resources. The
TALON mechanism is not designed to take the place of DoD's formal intelligence
reporting process.

　　　　Therefore, I hereby direct the implementation of policies and processes, as well as
the utilization of resources necessary to identify, report, share, and analyze non-validated
threat information in the United States through the use of the TALON system. Effective
immediately, all DoD intelligence, counterintelligence, law enforcement, and security
organizations that have the mission to collect force protection and threat information shall

U05646-03

identify, collect, and report the following categories of information, in accordance with existing policy and law, consistent with the TALON framework established by the Joint Staff Domestic Threat Working Group (see attachment): (1) non-specific threats to DoD interests; (2) suspected surveillance of DoD facilities and personnel; (3) elicitation attempts, suspicious questioning, or other suspected intelligence collection activities focused on DoD interests; (4) tests of security; (5) unusual repetitive activity; (6) bomb threats; and (7) any other suspicious activity and incidents reasonably believed to be related to terrorist activity directed against DoD personnel, property, and activities within the United States.

I hereby direct the Secretaries of the Military Departments, the Combatant Commanders, and Agency Directors to designate those components within their respective organizations that have the mission to collect and report this information and, further, to designate a single component within their respective organizations to assume the lead for distribution of this information. Once lead components are identified, they shall be identified to both the DoD Inspector General and the Assistant to the Secretary of Defense (Intelligence Oversight).

Upon identification of such information, lead components shall produce TALON reports and provide them to appropriate local military commanders and others responsible for installation security before the information is released outside the installation. Lead components that receive TALON reports shall ensure they are provided directly to the DoD Counterintelligence Field Activity (CIFA) and to other appropriate military commanders as secondary (info) recipients as necessary. CIFA will incorporate the information into a database repository and provide full database access to the Defense Intelligence Agency, Joint Intelligence Task Force-Combating Terrorism (JITF-CT) in order to support its terrorism warning mission. The CIFA and designated "lead components" in the Military Services, Combatant Commands, and Defense Agencies are authorized to retain TALON information as necessary to conduct their analysis missions. The Under Secretary of Defense, Intelligence (USD/I) is the designated overall lead official for this matter and will, therefore, validate the need of other DoD organizations for access to this information.

This policy remains in effect until superseded or until appropriate DoD policy on this subject is published or revised.

Paul Wolfowitz

Attachment:
As stated

SUBJECT: Attachment to DepSecDef Memo re: Collection, Reporting, and Analysis of Terrorist Threats to DoD Within the United States

BACKGROUND

The TALON system is designed to report anomalies, observations that are suspicious against the steady state context, and immediate indicators of potential threats to DoD personnel and/or resources. TALON reports are raw, non-validated information, which may or may not be related to an actual threat, and by their very nature, may be fragmented and incomplete. Information contained in TALON reporting is designed for use by Commanders at all levels that have force protection responsibilities and for analysts to use to help determine the aggregate terrorist threat to DoD people and resources.

TALON reports are of a tactical nature, with rapid reporting as the goal, and may be less refined than Intelligence Information Reports (IIRs). TALON reports are designed to capture raw threat data that does not meet IIR criteria. Critical to the reports is the proper documentation of the basic interrogatories (who – ALL PEOPLE INVOLVED, what, when, where, why, and how), the source's knowledge of these, and a clear definition of facts versus opinion (source's or reporter's).

TALON reports augment but are not designed to replace standard reporting mechanisms. IIRs, information files, operational files, and substantive investigations case files and associated reports are to be documented as directed by existing policies and directives.

As a general guide, to the maximum extent possible, TALON reports should be classified at the lowest possible level to ensure maximum distribution of the information. The use of the Law Enforcement Sensitive caveat and higher classifications should be kept to a minimum.

TALON information must be swiftly briefed locally to commanders and security officials so appropriate actions can be taken before this information is released outside the installation level. TALON reports are to be sent using automated information systems or via email attachment as a word document either on the NIPRnet for unclassified reports or on SIPRnet to respective Component Headquarters. Reports will be made as soon as possible after developing the information. Respective elements in designated Components will provide the TALON reports to the DoD Counterintelligence Field Activity (CIFA) as directed in the main policy memo of this attachment. The CIFA will ensure the JITF-CT has full access to the raw, non-validated information. Designated lead Service and Agency components will have access to the TALON database.

TALON REPORT GUIDE

TALON Report

CAUTION: TALONs are preliminary reports on ambiguous circumstances, and may contain incompletely evaluated information. TALONs are intended to alert commanders & staff to anomalies, potential terrorist indicators, or other FP issues.

1. **DATE**: (Date report is generated).

2. **LOCATION**: Location where the incident occurred.

3. **REPORTING UNIT**: Unit submitting the report.

4. **SEQUENCE NUMBER**: Your Component generated unique number.

5. **TALON CRITERIA**: Enter one of the following:

   a. Non-specific Threats. Threats received by any means, which contain a specific time, location or area for an attack against US forces, facilities or missions. This includes, but is not limited to, any event or incident, or series of events or incidents, which in and of themselves may indicate the potential for a threat to US forces, facilities, or mission, regardless of whether the threat posed is deliberately targeted or collateral.

   b. Surveillance: Any reported possible surveillance in which an attempt to record information or to use unusual means to monitor activities is observed. Such attempts may include use of cameras (either still or video), note taking, annotated maps or drawings, hand-drawn maps or diagrams, use of binoculars or other vision enhancing devices, or any reports from host nation security forces of possible surveillance of US assets.

   c. Elicitation. Any attempts to obtain security-related or military-specific information by anyone who does not have the appropriate security clearance and the need-to-know. Elicitation attempts may be made by mail, fax, telephone, by computer, or in person.

   d. Tests Of Security. Any attempts to measure security reaction times or strengths; any attempts to test or to penetrate physical security barriers or procedures; any attempts to acquire or duplicate uniforms, badges, passes, or other security related documents.

   e. Repetitive Activities. Any activities that meet one of the other TALON criteria and have occurred two or more times – the same activity by the same person and/or vehicle, within a 1 month period.

   f. Bomb Threats: Communication by any means specifically threatening to use a bomb to attack against US forces, facilities or missions.

   g. Suspicious Activities/Incidents: This category should **ONLY** be used if the TALON information **DOES NOT** meet any of the above criteria. Any activity/incident that does not specifically fit into the aforementioned six categories yet is believed to represent a force protection threat should be reported under this category. Examples of this include: issue resulting in the scrambling of homeland defense assets; thefts of material that could be used to manufacture false identification cards; thefts of military uniforms which may be used to gain access to a military installation, etc.

6. **RELEASABLE TO** Assign appropriate release information (REL to UK/CAN)

7. **CLASSIFICATION** Assign appropriate classification (FOUO, SECRET)

8. **CAVEAT**: Assign appropriate caveat ((LES, NOFORN)

9. **STATUS**: Choose Open/Unresolved, Closed/Unresolved or Closed/Resolved.

10. **ONE LINE TITLE**: Short title identifying what the TALON is about (i.e. Surveillance at Andrews AFB).

11. **SOURCE AND ASSESSMENT OF CREDIBILITY**: Who provided the information, how credible is the source, and why do you assess the source that way? (i.e. Desk Sgt, 82 SFS, direct access to information reported).

12. **DETAILS:** Who, What, When, Where, Why, and How. The most critical part of the report for the reader. Obtain all possible identification details of suspect(s) or suspected incident for further follow-up (including license plates). Be specific about what source said and about what source did not know (avoid second guessing by higher echelons). Use memory tools to aid source in remembering details (mild interrogation). For example, one tool all Army personnel are trained in, down to the troop level, is SALUTE. Size (size of suspicious element - e.g. "2 people"); Activity (what was going on - e.g. "drove by guard gate slowly"); Location (where did it happen - e.g. "guard post 3"); Unit (identification of unit involved - e.g. "local contractor hired TCN"); Time (when

did it happen - e.g. "20:00 hours, 2 January 20__"); Equipment (what were they carrying, driving, etc. - e.g. "in 1990 white Caprice, with binoculars, writing notes on an aviator knee pad").

13. **COUNTRIES** What countries does the information in the TALON relate to.

14. **PERSONS BRIEFED LOCALLY**: Who was briefed locally, and when were they notified of the incident, (i.e.: Base Commander, 82 SFS/CC, Phoenix JTTF, etc).

15 **ACTIONS TAKEN**: What investigative steps have already been accomplished.

16. **ACTIONS PENDING**: What investigative steps are you involved in or do you have planned to bring the incident to closure (running license plate checks, interview another witness, etc.)

17. **SUMMARIZE TALON**: Two to three sentences giving the basic summary of what the TALON is about. This is not a regurgitation of the details but a simple summary – should not contain any specific information. (i.e. Unknown individual observed photographing front gate of Andrews AFB. When approached, he left and a license plate was recorded. The license plate was identified as being invalid so no further information could be obtained). The specifics should be in the detail section. This is the short summary that, along with the one line title, if posted to the face of the webpage can gain the readers attention.

18. **COMMENTS**: Any information the reporting unit wants to convey and maintain as internal organization comments. Fully identify information sources here.

19. **PERSONS INVOLVED**: Fill-in the blocks – SUBJECTS, WITNESSES, INCIDENTALS