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

SUBJECT: Threats to the Department of Defense (DoD)

The TALON Reporting System is an innovative initiative to document unfiltered and non-validated potential threat information about suspicious activity linked to possible international terrorist threats to DoD personnel and resources that might have otherwise gone unreported. This information is reported by concerned citizens and Department personnel or obtained through information sharing with civilian law enforcement agencies. The program has been productive. It has detected international terrorist interest in specific military bases and has led to and supported counterterrorism investigations.

The Department has completed the review and assessment of the TALON Reporting System addressed in my memorandum of January 13, 2006, "Retention and Use of Information for the TALON System." This review confirmed that the TALON Reporting System should be used only to report information regarding possible international terrorist activity and concluded that all TALON reports should be retained in accordance with DoDD 5240.1-R, "Activities of DoD Intelligence Components That Affect United States Persons," dated December 1982.

To ensure the continued effectiveness of the TALON Reporting System, I am directing all DoD components that use the TALON Reporting System to comply with the procedures listed in Enclosure (1) and to ensure the information included in their TALON reports meet the criteria for reporting described in Enclosure (1).
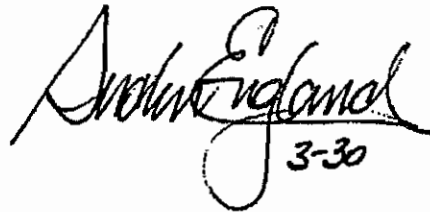
This Memorandum provides interim guidance. Given the importance of capturing threat information in protecting the Department's personnel, property and facilities, I am Directing the Under Secretary of Defense for Intelligence (USD(I)) to convene a working group to examine the integration of threat information across the DoD intelligence, counterintelligence, law enforcement, force protection and security communities. The

USD(I) will report the findings of this working group to me by Sep 15, 2006. The interim guidance contained in this memorandum will remain in effect until the above described working group's findings are published and permanent TALON Reporting System policy is promulgated.

By this memorandum I am also directing the Assistant to the Secretary of Defense (Intelligence Oversight), on an annual basis, to review the TALON Reporting System and to provide a report to the USD(I) with the status of the first review within 60 days. The USD(I) and the DoD Counterintelligence Field Activity (CIFA) will work with the DoD Inspector General on its ongoing audit of the TALON Reporting System.

The May 2, 2003, Deputy Secretary of Defense Memorandum, titled, "Collection, Reporting and Analysis of Terrorist Threats to DoD Within the United States," (Enclosure 2) required the identification of "lead components" within the Military Departments to distribute TALON reporting from their respective Departments. I hereby direct each lead component to provide to CIFA, by May 12, 2006, a copy of its guidance to implement the process set forth in Enclosure (1). CIFA will review each Department's guidance to insure it conforms with the process in Enclosure (1) and will provide a status report to the Deputy Under Secretary of Defense (Counterintelligence and Security) by May 30, 2006.

Gordon England

3-30

Enclosures:
1. TALON REPORTING SYSTEM PROCEDURES
2. Deputy Secretary of Defense memo of May 2, 2003, Subject: "Collection, Reporting and Analysis of Terrorist Threats to DoD Within the United States"

Enclosure (1) to Deputy Secretary of Defense Memorandum, "Threats to the Department of Defense"

TALON REPORTING SYSTEM PROCEDURES

- The guidance for the TALON Reporting System as provided in Deputy Secretary of Defense Wolfowitz's memo of May 2, 2003, "Collection, Reporting and Analysis of Terrorist Threats to the Department of Defense (DoD) Within the United States," (Enclosure (2)) remains in force. This document updates and clarifies that guidance.

- The TALON Reporting System is the Department's mechanism to gather, share, compile, and retain unfiltered non-validated threat or suspicious activity information possibly linked to international terrorist activities posing a potential threat to DoD personnel and resources both domestically and abroad.

REPORTING TALON INFORMATION

A proposed TALON report must meet one of the following seven criteria (the criteria remain substantially the same as in the DepSecDef memo of May 2, 2003):

1. Specific or non-specific threats to DoD interests.

2. Suspected surveillance of DoD facilities or 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.

7. Any other suspicious activity and incidents reasonably believed to be related to international terrorist activity directed against DoD personnel, property, and activities within the United States or abroad.

- An appropriate level supervisor in each DoD organization authorized to submit. TALON reports shall review each proposed report prior to submission to the Counterintelligence Field Activity (CIFA) to ensure it meets one of the reporting criteria listed above and one of the following detailed criteria descriptions:

1. Specific or Non-Specific Threats: Specific threats are threats received by any means, which contain a time, location or area for an attack against US forces, facilities, or missions. Non-specific threats include, but are 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.

2. 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.

3. 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.

4. Test of Security: Any attempts to measure security reaction times or strength; any attempts to test or penetrate physical security barriers or procedures; any attempts to acquire or duplicate uniforms, badges, or other security related documents.

5. 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 one month period.

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

7. 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 potential threat should be reported under this category. Examples of this include: an anomaly noticed resulting from the deployment of homeland defense assets; theft of material that could be used to manufacture false identification cards; thefts of military uniforms which may be used to gain access to military installation, etc.

• If information meets the reporting criteria set forth above, the reporting organization is deemed to hold a reasonable belief that there is a nexus between the information

Enclosure 1

and "international terrorist activity," and it may be forwarded to CIFA as a TALON report for inclusion in the Cornerstone database.

- If a TALON reporting entity determines that a TALON report is of interest to local command authorities, law enforcement (DoD and/or non-DoD) or homeland defense entities, it may share the information in the report with those organizations via established lines of communication.

- CIFA will conduct a review of all TALON reports submitted to the Cornerstone database to confirm they meet the reporting criteria. CIFA shall immediately remove from the database any report that does not meet the criteria. CIFA will notify the submitter of the TALON report of the removal and verify the reporting entity also purges the TALON report from its system.

- Credible information about a possible international terrorist threat sufficient to warrant an investigation must be referred to the proper investigative agency immediately by the reporter and/or CIFA.

- Information that is responsive to existent intelligence or counterintelligence DoD collection requirements must be reported in Intelligence Information Reports and not entered into the TALON Reporting System.

RETAINING TALON REPORTS

- Only DoD intelligence and counterintelligence organizations may retain TALON reports. DoDD 5240.1-R, "Activities of DoD Intelligence Components That Affect United States Persons," dated December 1982 governs the retention of US person information in TALON reports. Identifying US person information in TALON reports and in the Cornerstone database may be retained indefinitely if there is a reasonable belief the person is engaged in or about to engage in international terrorist activities. If this reasonable belief cannot be established within 90 days from the time the information is collected, the identifying US person information may not be retained by any intelligence or counterintelligence organization. CIFA will remove the US person information from the Cornerstone database and notify the submitting component of the removal. The submitting component must also remove the US person information from its system and advise CIFA of the removal within 5 days of receiving the notification from CIFA.

- However, the US person information may be disseminated by CIFA to a law enforcement entity prior to its removal from the Cornerstone database if the information is of interest to law enforcement and meets legal requirements for transfer of the information. Law enforcement organizations may request from CIFA, and

CIFA may provide to them, any TALON reports held for which the law enforcement organization has a legitimate legal requirement.

ANALYSIS OF TALONS

- Any organization that identifies possible international terrorist activity based upon TALON Reporting System analysis will immediately notify the appropriate law enforcement agencies, command authorities and CIFA.

- Any organization that determines a previously submitted TALON report is not linked to possible international terrorist activity will immediately notify CIFA so that CIFA can remove the report from the Cornerstone Database. CIFA will notify TALON Reporting System users of the reports that it deletes from the Cornerstone database, based on its own analysis or that of any other organizations, and the users must notify CIFA within 5 days of receiving the notification that they have also deleted the report from their system(s). Within 5 days of receiving a notification from CIFA, the TALON reporting entity must also notify any command authorities, law enforcement or homeland defense entity that received the information from the reporter that the information is not linked to possible international terrorist activity.

ADMINISTRATIVE MATTERS

- CIFA is responsible for the maintenance of the Cornerstone database that is the central DoD repository for TALON reports.

- CIFA will continue to ensure only authorized personnel and organizations have access to the TALON Reporting System and Cornerstone database.

- Although the TALON Reporting System is focused on DoD facilities, interests or personnel, should non-specific information be received about suspicious activities possibly linked to international terrorist actions against non-DoD personnel, activities or facilities, that information should be provided to the appropriate local authorities.

Enclosure 1