



DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
FREEDOM OF INFORMATION/PRIVACY OFFICE
FORT GEORGE G. MEADE, MARYLAND 20755-5995

REPLY TO
ATTENTION OF:

Freedom of Information/
Privacy Office

AUG 24 2009

Ms. Marcia Hofmann
Electronic Fronteir Foundation
1875 Connecticut Avenue, Northwest
Suite 650
Washington, DC 20009

Dear Ms. Hofmann:


This is in further response to your Freedom of Information Act (FOIA) request of November 15, 2006, for records relating to "TALON" reports and supplements our response of July 9, 2009.

Coordination has been completed and the records have been returned to this office for our disposition. We have reviewed the records and determined the records are releasable to you. The records are enclosed for your use.

There are no assessable FOIA fees for processing this request.

If you have any questions regarding this action, feel free to contact this office at 1-866-548-5651 (Press 2/Press 6), or email the INSCOM FOIA office at: INSCOM_FOIA_ServiceCenter@mi.army.mil and refer to case #542F-09.

Sincerely,


Susan J. Butterfield
Director
Freedom of Information/Privacy Office
Investigative Records Repository

Enclosure

Enclosure (1) to Deputy Chief of Staff, G-2 Memorandum, "Interim Implementation Guidance for Army Intelligence and Counterintelligence Activities Regarding TALON Reporting"

ARMY INTERIM TALON IMPLEMENTATION GUIDANCE

1. (U) Reporting TALON Information.

a. (U//FOUO) Agency Review Process: The report drafter (Agent) will compose a new TALON report and save it as a draft TALON in the template provided in a restricted queue on the Cornerstone database web page. The report will include the mandatory fields identified on the template and a comment field that will require the reporting agency's reviewer's authorization. Army counterintelligence and intelligence activities will establish an internal review process for TALONs. Once this review is annotated on the template, the draft will then be ready for review by the Counterintelligence Field Activity (CIFA) and released to the Cornerstone database by CIFA. The Army Counterintelligence Information Center (ACIC) will establish specific guidelines for submission by US Army Military Intelligence (MI) activities of TALONs with US person information.

(1) (U//FOUO) This process will allow for the reporting agency, and the ACIC, 902d MI Group to review all TALON reports containing US person information submitted by Army MI activities prior to their release to the CIFA Cornerstone database. The ACIC is the only Army MI activity authorized to release TALON reports containing US person information to CIFA for inclusion in the Cornerstone database.

(2) (U//FOUO) Release Authority (CIFA): CIFA will be the final release authority for TALON reporting into the Cornerstone database.

b. (U//FOUO) Information about a possible international terrorist threat that is sufficiently credible to warrant an investigation must be referred to the proper investigative agency immediately, in addition to reporting via the TALON reporting system. Access to that report will be restricted to users with a need-to-know.

c. (U//FOUO) Information that is reportable under the provisions of AR 381-12 will be reported into SAEDA channels. Information that is responsive to intelligence or counterintelligence standing collection requirements will be reported in Intelligence Information Reports and will not be entered into the TALON Reporting System.

d. (U//FOUO) Organizations reporting TALON information must have a reasonable belief that there is a nexus between the information and "international terrorist activity" that may pose a threat to DoD personnel or resources.

e. (U) Criteria for TALON reporting.

(1) (U//FOUO) Specific or nonspecific threats to DoD interests.

(2) (U//FOUO) Suspected surveillance of DoD facilities or personnel.

(3) (U//FOUO) Elicitation attempts, suspicious questioning, or other suspected intelligence collection activities focused on DoD interests.

(4) (U//FOUO) Tests of security.

(5) (U//FOUO) Unusual repetitive activity.

(6) (U//FOUO) Bomb threats.

(7) (U//FOUO) 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.

(U) Note: Although this program is focused on DoD facilities, interests or personnel, should nonspecific 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 locally affected command and law enforcement (LE) authorities.

f. (U) TALON reports will not be used to report on US persons exercising their constitutionally protected freedoms of speech and assembly.

2. (U) Retention of TALON reports by Army Intelligence and Counterintelligence activities:

a. (U) No Army MI asset (including the ACIC) will maintain an internal TALON database.

b. (U) The ACIC is the only Army intelligence asset authorized to maintain information gleaned from TALON reports. The ACIC may retain information gleaned from TALON reports for as long as necessary for analytic purposes; however, if a TALON report contains identifying US person information the following applies:

(1) (U) Identifying US person information in TALON reports may be retained as long as necessary if there is a reasonable belief the person is engaged in or about to engage in international terrorist activities.

(2) (U) If this reasonable belief cannot be established within 90 days from the time the information is reported by the Army MI activity, the ACIC must notify CIFA to delete the TALON report containing US person information.

c. (U) The ACIC will immediately notify Army MI activity reporters whether any TALON reports containing US person information will be removed from the TALON database.

3. (U) Interaction between Army MI and LE entities concerning TALON reportable information:

a. (U) Army LE entities (MP/CID field elements) that acquire any possible TALON related information will input the information into the Joint Protection Enterprise Network system (JPEN) and also pass any TALON reports with US person information to the local MI elements for information purposes.

b. (U) Other information acquired by LE entities that does not meet the TALON criteria as outlined in paragraph 1e, will be processed according to LE entities' internal procedures.

c. (U) ACIC analysts will review all reports prior to submission to the TALON Cornerstone database. Any report that is determined to be law enforcement or domestic extremist related rather than international terrorist related will not be entered into the TALON Cornerstone database; however, the report will be given to the CID agent assigned to the ACIC for processing through LE channels.

d. (U) At all levels, information acquired by MI organizations that is of LE interest will be passed to LE authorities through established channels.

e. (U) When the creator of a TALON report identifies possible terrorist activity he will immediately notify his superior who will in turn notify law enforcement agencies, command authorities and CIFA.

f. (U) When the ACIC identifies possible terrorist activity through analysis, the ACIC will immediately notify law enforcement agencies, command authorities and CIFA.

4. (U) Intelligence oversight training. All Army intelligence and intelligence support assets who submit, process, and coordinate TALON reports will conduct annual training focused on the policies and procedures regarding collection, retention, and dissemination of US Persons information.

DEPARTMENT OF THE ARMY
OFFICE OF THE DEPUTY CHIEF OF STAFF, G-2
Responses to DoD Integrated Threat Working Group Task

USDI Integrated Threat Working Group Task

Task: Identify issues concerning the current DoD TALON policy and provide recommendations to those issues.

(1) Issue: Ambiguities in linking the criteria to a nexus to international terrorism.

- Although the 30 Mar 06 DEPSECDEF memorandum, subject: "Threats to the Department of Defense" stipulates that TALON reports must have a nexus to international terrorism, and defines those activities that may be reported as having a nexus to international terrorism solely because they meet the criterion listed in the memorandum causes confusion in the field.
- DEPSECDEF memorandum states: If information meets the following criteria (Specific or non-specific threats; surveillance; elicitation; Test of security; Repetitive activities; Bomb threats; Suspicious activities/incidents), the reporting organization is deemed to hold a reasonable a reasonable belief that there is a nexus between the information and international terrorism activity.
- As an example: A Fort Belvoir school bus full of kids taking pictures of Fort Belvoir probably does not constitute a foreign nexus (although the ambiguities in the language of the DEPSECDEF memorandum says it does) but some "tourists" taking photos of Fort Belvoir could reasonably constitute a nexus.

Recommendation: The verbiage in enclosure 1 to the DEPSECDEF memorandum be changed to read: "If information meets the reporting criteria above, and there is a reasonable belief of trained law enforcement or military intelligence personnel that a nexus between the information and international terrorism activity could exist, it may be forwarded to CIFA as a TALON report for inclusion in the Cornerstone database."

(2) Issue: Sharing Information between reporting mechanisms

- Currently law enforcement (LE) entities report TALON information via the Joint Protection Enterprise Network ((JPEN) and Army Military Intelligence (MI) entities report TALON information via the

Cornerstone database. This especially applies to the Army because there is a true separation between LE and MI (Air Force and Navy bifurcate their information between the two systems.) The purpose of the TALON reporting system being two fold (1) collect, and share non-validated threat information between LE and MI, and (2) subject that information to careful analysis. The purpose of the TALON report is to document and immediately disseminate potential threat information.

- The JPEN is an unclassified system available for use by all Services; reports entered into this system are immediately available to all Services LE assets utilizing the system. This provides instantaneous sharing of threat information with all posts, bases, and facilities.
- The Cornerstone database is limited to those activities that have classified systems, which in-turn limits the dissemination of threat information. However, the Cornerstone database provides access to information on a system that can subject that information to careful analysis.

Recommendation: All elements who produce TALON reports (including Army MI) should utilize the JPEN for reporting purposes. This will allow for instantaneous sharing of potential threat information with all posts, bases, and facilities. For purposes of analysis, CIFA would extract data from JPEN that meets the criteria for TALON reports and transfer that information to the Cornerstone database.

(3) Issue: Retention of Information Reported through the TALON System

- As per the 30 Mar 06, DEPSECDEF memorandum, TALON information will be retained per DODD 5240.1. This works well for information reported directly to the CIFA TALON Cornerstone database, however, this is not the case for information reported through the JPEN. NORTHCOM maintains a policy of purging all reports reported to JPEN at the 90-day point.
- Army LE entities (OPMG and CID) have both expressed concerns regarding the loss of information reported through the JPEN system. Although CIFA extracts reports from the JPEN that are deemed to meet TALON reporting criteria, not all reports will be extracted. However, NORTHCOM currently purges all data within JPEN that reaches the 90-day point. As a result, the data that is not captured by CIFA for inclusion in the Cornerstone database is lost. This information, although not specifically meeting TALON reporting criteria may be of use to the LE community.

Recommendation: USD(I) better define and promulgate guidance for the retention of information submitted to the JPEN.



**DEPARTMENT OF DEFENSE
OFFICE OF FREEDOM OF INFORMATION
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155**

26 JUN 2009

Ref: 07-F-0335

Ms. Marcia Hoffman
Staff Attorney
Electronic Frontier Foundation
1875 Connecticut Ave., N.W.
Suite 650
Washington, DC 20009

Dear Ms. Hoffman:

This is the final response to your November 15, 2006, Freedom of Information Act (FOIA) request, for records related to a memorandum issued by the Deputy Secretary of Defense, which directed certain DoD personnel and components to take steps to improve oversight of the TALON Reporting System. Specifically, you requested the following agency records for the time period of March 2006 to the present: (1) all reports, statements, memoranda or other documents created by the working group tasked to "examine the integration of threat information across the DoD intelligence, counterintelligence, law enforcement, force protection and security communities;" (2) "any reports from the Assistant to the Secretary of Defense (Intelligence Oversight) on the status of TALON Reporting System reviews;" and, (3) "copies of each Military Department's guidance for implementing TALON reporting procedures" and "all reports from CIFA to the Deputy Under Secretary of Defense (Counterintelligence and Security) on TALON reporting guidelines."

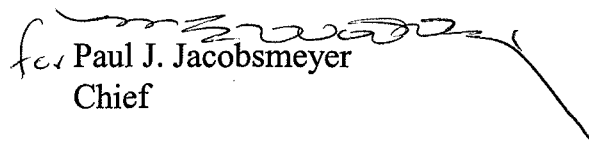
The Office of the Assistant to the Secretary of Defense for Intelligence Oversight (ATSDIO), the Counterintelligence Field Activity (CIFA), and the Office of the Under Secretary of Defense for Intelligence (OUSDI) conducted searches and located 22 documents responsive to your request. Michael Reheuser, an Initial Denial Authority (IDA) for the Office of the General Counsel, determined that one document, totaling three pages, is exempt from release in its entirety pursuant to 5 U.S.C. § 552(b)(5), which applies to attorney work-product deliberative and pre-decisional privilege. Ten documents are under the purview of other agencies and are being referred to those agencies for review and direct response to you. If you have any questions regarding the processing of these documents, you may contact the appropriate agency at the address provided on the attached document.

The remaining 11 documents are provided as responsive to your request. William J. Kane, an IDA for the Joint Staff, William Dugan, an IDA for ATSDIO, Deborah Parker, an IDA for CIFA, and John Smith, an IDA for OUSDI, have reviewed the

documents and determined that the redacted portions are exempt from release pursuant to 5 U.S.C. § 552(b)(2), which pertains to purely internal agency practices and 5 U.S.C. § 552(b)(5), which applies to attorney work-product deliberative and pre-decisional privilege. The remaining information is being withheld pursuant to 5 U.S.C. § 552(b)(6), which pertains to information the release of which would constitute a clearly unwarranted invasion of the personal privacy of third parties.

If you are not satisfied with this action, you may submit an administrative appeal to James Hogan, Chief, Policy, Appeals and Litigation Branch, Office of Freedom of Information, 1155 Defense Pentagon, Washington, D.C. 20301-1155. Your appeal should be postmarked within 60 calendar days of the date of this letter, should cite to case number 07-F-0335, and should be clearly marked "Freedom of Information Act Appeal." There are no fees associated with this response in this instance.

Sincerely,


for Paul J. Jacobsmeyer
Chief

Enclosures:
As stated.

Contact Information for Agencies Reviewing Responsive Documents

Documents #6 & #10

Department of the Navy
Office of the Chief of Naval Operations
DNS-36
2000 Navy Pentagon
Washington, DC 20350-2000

Documents #8 & #22

Department of the Air Force
AF/ILCSE
1500 Wilson Blvd.
Arlington, VA 22209

Documents #9 & #20

Department of the Army
Attn: AHRC-PDD-FP
Freedom of Information & Privacy Acts Division
7701 Telegraph Road
Alexandria, VA 22315-3860

Documents #16 & #17

Inspector General of the Department of Defense
Chief, FOIA/PA Office
400 Army Navy Drive, Rm. 201
Arlington, VA 22202-4704

Document #18

Defense Security Service
Chief, Office of FOIA & Privacy
1340 Braddock Place
Alexandria, VA 22314-1651

Document #19

U.S. Northern Command
USNORTHCOM FOIA Officer
250 Vandenberg Street, Suite B016
Peterson Air Force Base, CO 80914

~~UNCLASSIFIED/FOR OFFICIAL USE ONLY~~

**Assistant to the Secretary of Defense for
Intelligence Oversight (ATSDIO)**



**Intelligence Oversight Review of the
TALON Reporting System**

May 25, 2006

This Review was directed by Deputy Secretary of Defense Memorandum, March 30, 2006, Subject: "Threats to the Department of Defense."

~~UNCLASSIFIED/FOR OFFICIAL USE ONLY~~

TABLE OF CONTENTS

Executive Summary

Issues and Recommendations

Discussion:

1. Scope and Methodology (FOUO)
2. Background on the TALON Reporting System and the Problems with the Portico-Cornerstone Database (FOUO)

3. (b)(5)

4.

5.

6.

7.

8.

9.

Attachments:

- A. Deputy Secretary of Defense Memorandum, dated March 30, 2006, Subject: "Threats to the Department of Defense"
- B. DoD General Counsel Memorandum, dated January 25, 2006, Subject: "Application of DoDD 5240.1-R to the Talon Reporting System and Cornerstone Database"
- C. Memorandum from the Vice Chief of Naval Operations to the Under Secretary of Defense for Intelligence, dated March 16, 2006, Subject: "Protecting DoD Resources"

References:

1. Executive Order 12333, "United States Intelligence Activities," December 4, 1981
2. DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1982

May 25, 2006

ATSD(IO) REVIEW OF TALON REPORTING SYSTEM

EXECUTIVE SUMMARY

(U/~~FOUO~~) The Deputy Secretary of Defense March 30, 2006 Memorandum, Subject: "Threats to the Department of Defense" (TAB A) directed that the TALON Reporting System should be used only to report information regarding possible international terrorist activity and that all TALON reports should be retained in accordance with Intelligence Oversight regulations. (b)(5)

(b)(5)

(b)(5)

ISSUES AND RECOMMENDATIONS

(U/~~FOUO~~) (b)(5)

(b)(5)

(U/~~FOUO~~) (b)(5)

(b)(5)

(U/~~FOUO~~) **ISSUE 1A:** Deputy Secretary of Defense March 30, 2006 Memorandum, Enclosure 1 provides: "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 DoD Within the United States," (Enclosure (2)) remains in force. This document updates and clarifies that guidance. (Emphasis added.) (b)(5)

(b)(5)

(b)(5)

(U/FOUO) (b)(5)

(b)(5)

(U/FOUO) (b)(5)

(b)(5)

(U/FOUO) (b)(5)

(b)(5)

(U/FOUO) (b)(5)

(b)(5)

(U/FOUO) (b)(5)

(b)(5)

UNCLASSIFIED/FOR OFFICIAL USE ONLY

(U/FOUO) ISSUE 4: The Joint Protection Enterprise Network (JPEN) system is a law enforcement/force protection database maintained by U.S. Northern Command (NORTHCOM). (b)(5)

(b)(5)

(b)(5)

(U/FOUO) (b)(5)

(b)(5)

(U/FOUO) (b)(5)

(b)(5)

(U/FOUO) (b)(5)

(b)(5)

(b)(5)

(U/FOUO) (b)(5)

(b)(5)

(b)(5)



(U//FOUO) (b)(5)

(b)(5)



(U//FOUO) (b)(5)

(b)(5)



(U//FOUO) (b)(5)

(b)(5)



(b)(5)

(U//~~FOUO~~) Questions regarding the collection, retention, and dissemination under DoD 5240.1-R have customarily been resolved by the ATSD(IO) in conjunction with the DoD GC. The ATSD(IO) has consistently maintained that the recipient of intelligence information is responsible for determining if retention of that information is compliant with the provisions of DoD 5240.1-R.

(U//~~FOUO~~) (b)(5)

(b)(5)

(U//~~FOUO~~) **1. Scope and Methodology.**

(U//~~FOUO~~) The Deputy Secretary of Defense Memorandum March 30, 2006, Subject, "Threats to the Department of Defense (DoD)" directed the ATSD(IO) to review the TALON Reporting System and provide the results to the USD(I) within 60 days. The Acting ATSD(IO) and two senior inspectors from the ATSD(IO) staff (hereinafter the "ATSD(IO) Team") conducted the review. (b)(5)

The Memorandum directed that the TALON Reporting System should be used (1) only to report information regarding possible international terrorist activity, and (2) that all TALON reports should be retained in accordance with Intelligence Oversight regulations.

(U//~~FOUO~~) The ATSD(IO) Team visited the Counterintelligence Field Activity (CIFA), Crystal City, Virginia, twice. During the second visit to CIFA, the ATSD(IO) Team reviewed a number of TALON Reports in the TALON database and discussed with CIFA analysts how they analyzed the TALON Reports. One team member visited CIFA West, located in Colorado Springs, Colorado.

(U//~~FOUO~~) Since the military services together submit more than 98% of the TALON reports in the TALON database, the ATSD(IO) Team focused on them during this review. The ATSD(IO) Team met with representatives of Army intelligence, counterintelligence, and law enforcement; Naval Criminal Investigative Service (NCIS),

and Air Force Office of Special Investigations (AFOSI). They are the organizations who submit items into the TALON Reporting System.

(U//~~FOUO~~) At each organization visited, the ATSD(IO) Team reviewed internal operating procedures and the flow of TALON Reporting from initial report writing, through internal review, and on to receipt by CIFA of the TALON Report and entry into the Portico-Cornerstone data base. The ATSD(IO) Team also reviewed how each organization applied the Intelligence Oversight regulations to their reporting process. The ATSD(IO) Team received complete cooperation from all the organizations contacted; we were impressed by their frankness and openness.

(U//~~FOUO~~) 2. Background on the TALON Reporting System and the Problems with the Portico-Cornerstone Database

(U//~~FOUO~~) The Deputy Secretary of Defense established the TALON Reporting System by Memorandum dated May 2, 2003, "Collection, Reporting, and Analysis of Terrorist Threats to DoD Within the United States." The purpose of the system was to document and immediately disseminate potential threat information to DoD personnel, facilities, and resources. It was based on a system originally developed by the Air Force Office of Special Investigations. TALON Reporting was not designed to take the place of DoD's formal intelligence reporting process. Instead, the TALON Reporting System was designed to collect and share non-validated domestic threat information among intelligence, counterintelligence, law enforcement and force protection entities and subject that information to careful analysis for indications of foreign terrorist activity. In addition to reporting to local military commanders and others responsible for installation security, TALON Reports were to be provided to the Counterintelligence Field Activity (CIFA). CIFA incorporated the information into a database and made it available to others so they could analyze the information. CIFA also analyzed the information.

(U//~~FOUO~~) The Deputy Secretary of Defense Memorandum dated May 2, 2003 identified seven criteria for reporting:

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
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.

(U//FOUO) The TALON Reports are maintained by CIFA in a database called Portico-Cornerstone. It is available on the SIPRNET at the SECRET level and access is controlled by CIFA with a password system.

(U//FOUO) Extensive media coverage, beginning in December 2005, revealed that information about demonstrations, protests and protest groups, and other non-terrorist related issues was contained in TALON Reports and retained in the Portico-Cornerstone database. In addition, information identifying U.S. Persons who had no connection to international terrorism was found in the database. The Deputy Secretary of Defense Memorandum dated January 13, 2006, Subject: Retention and Use of Information in the TALON System, directed that all reports in the TALON database be reviewed by January 17, 2006, to identify any reports that should not be in the database [and remove them]. (Note: This review by CIFA of reports in the Portico-Cornerstone database had been earlier directed by the Under Secretary of Defense for Intelligence and had been underway since mid-December 2005.)

(U//FOUO) Well before the media publicity in December 2005, CIFA had determined in July 2005 that better oversight of the system was required. In August 2005, CIFA produced standard operating procedures. Beginning September 1, 2005, CIFA West began to review all incoming TALON Reports for oversight purposes.

(U//FOUO)

(b)(5)



(U//FOUO)

(b)(5)

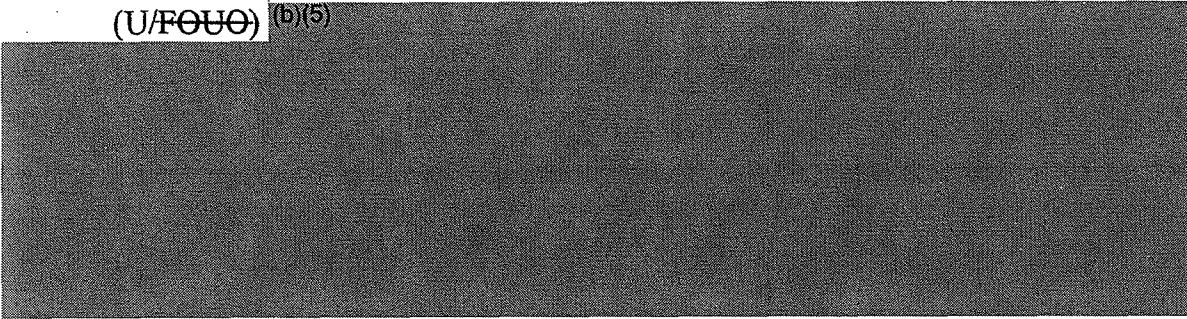


(U//FOUO)

(b)(5)



(U//~~FOUO~~) (b)(5)



(U//~~FOUO~~) 3. **Disconnects Between the Deputy Secretary of Defense March 30, 2006 Memorandum and Enclosure 1 to the Memorandum**

(U//~~FOUO~~) The March 30, 2006, Deputy Secretary of Defense Memorandum Subject, "Threats to the Department of Defense (DoD)" directed that the TALON Reporting System should be used only to report information regarding possible international terrorist activity and that all TALON Reports should be retained in accordance with Intelligence Oversight regulations - DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1982. This is clear direction for the DoD intelligence community.

(U//~~FOUO~~) (b)(5)



(U//~~FOUO~~) Enclosure 1 provides: "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 DoD Within the United States," (Enclosure (2)) remains in force. This document updates and clarifies that guidance. (Emphasis added.)

(U//~~FOUO~~) 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. (Emphasis added.)

(U//~~FOUO~~) A proposed TALON report must meet one of the seven criteria (the criteria remain substantially the same as in the DepSecDef memo of May 2, 2003): [The March 30, 2006 Memorandum changes in the criteria are highlighted in **bold print**.]

1. **specific or non-specific threats to DoD interests**
2. **suspected surveillance of DoD facilities and 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. "**

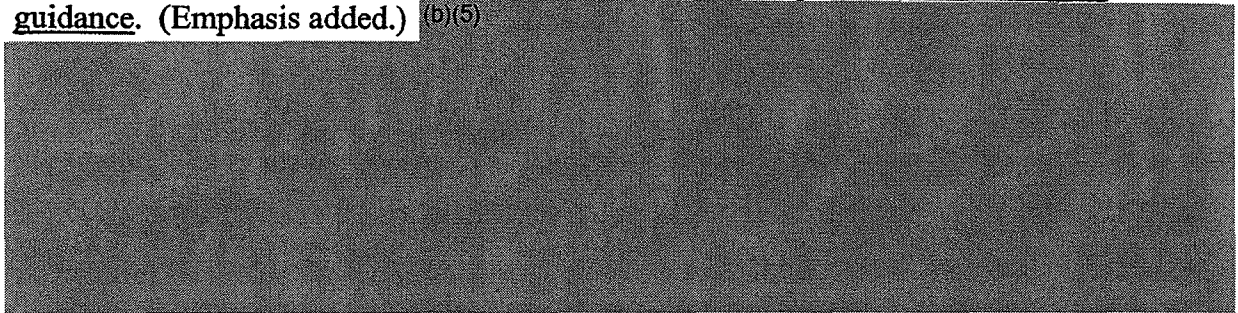
(U//~~FOUO~~) (b)(5)



(U//~~FOUO~~) (b)(5)



(U//~~FOUO~~) In addition, Deputy Secretary of Defense March 30, 2006 Memorandum, Enclosure 1 provides: "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 DoD Within the United States," (Enclosure (2)) remains in force. This document updates and clarifies that guidance. (Emphasis added.) (b)(5)



~~(U/FOUO)~~ 4. CIFA and CIFA West Responsibilities

~~(U/FOUO)~~ March 30, 2006, Deputy Secretary of Defense Memorandum Subject, "Threats to the Department of Defense (DoD)," Enclosure 1, TALON Reporting System Procedures directs CIFA to do the following:

~~(U/FOUO)~~ 1. Review all TALON reports submitted for entry into the Portico-Cornerstone database to confirm they meet the reporting criteria. Any report that does not meet the criteria should be removed.

~~(U/FOUO)~~ 2. Remove from the database any report that does not meet the reporting criteria, notify the submitter of the TALON report of the removal and verify that the reporting entity also purges the TALON report from its system.

~~(U/FOUO)~~ 3. CIFA is responsible for the maintenance of the Portico-Cornerstone database that is the central DoD repository for TALON reports.

~~(U/FOUO)~~ 4. Ensure only authorized personnel and organizations have access to the TALON Reporting System and Portico-Cornerstone database. CIFA will accomplish this by registering authorized users.

~~(U/FOUO)~~ ~~(b)(5)~~



~~(U/FOUO)~~ 5. The Portico-Cornerstone Database Software

~~(U/FOUO)~~ ~~(b)(5)~~



~~(U/FOUO)~~ ~~(b)(5)~~



(b)(5)

(U//FOUO) (b)(5)

(b)(5)

(b)(5)

(U//FOUO) 6. Army TALON Reporting System

(U//FOUO) The Army has identified the Deputy Chief of Staff, G2 (Intelligence) as the Executive Agent for TALON Reporting. The Army has changed its procedures for TALON Reporting by Army counterintelligence and intelligence organizations in response to the March 30, 2006 Deputy Secretary of Defense Memorandum. Unlike the Navy and Air Force, Army law enforcement and counterintelligence organizations are separate. (b)(5)

(b)(5)

(U//FOUO) (b)(5)

(b)(5)

(U//FOUO) (b)(5)

(b)(5)

(U//FOUO) (b)(5)

(b)(5)

(b)(5)



(U//FOUO) 7. Navy and Marine Corps TALON Reporting System

(U//FOUO) The Secretary of the Navy has identified the Naval Criminal Investigative Service (NCIS) as the Executive Agency responsible for TALON reporting within the Department of the Navy including the Marine Corps. Suspicious incidents are reported to the local NCIS agent who writes a TALON Report within 24 hours of notification of the incident. The reporting unit of the NCIS agent who prepared the initial report reviews it to ensure compliance with the Deputy Secretary of Defense March 30, 2006 Memorandum and DoD 5240.1-R. The TALON report is then sent by SIPRNET to the NCIS Headquarters Multiple Threat Alert Center (MTAC). MTAC provides a secondary review and provides the TALON Report to CIFA for entry into the Portico-Cornerstone database. TALON updates are provided to CIFA when necessary. MTAC also maintains the information in its databases - which are "non-TALON" databases.

(U//FOUO) (b)(5)



(b)(5)

(U//FOUO) (b)(5)



(b)(5)

(b)(5)

(U//~~FOUO~~) Questions regarding the collection, retention, and dissemination under DoD 5240.1-R have customarily been resolved by the ATSD(IO) in conjunction with the DoD GC. The ATSD(IO) has consistently maintained that the recipient of intelligence information is responsible for determining if retention of that information is compliant with the provisions of DoD 5240.1-R. (b)(5)

(b)(5)

(U//~~FOUO~~) 8. Air Force TALON Reporting System

(U//~~FOUO~~) TALON Reporting had been treated as law enforcement reporting in the Air Force. In order to comply with the Deputy Secretary of Defense March 30, 2006 Memorandum, the Air Force Office of Special Investigations (AFOSI), the organization responsible for TALON reporting in the Air Force, has changed its procedures for TALON Reporting. AFOSI field units will continue to report suspicious events to the Headquarters AFOSI Global Watch Center. The Global Watch Center will determine if any field reports meet the TALON reporting criteria. For those reports that do, the Global Watch Center will generate the TALON Report and publish it to the Eagle Watch web page. CIFA retrieves the TALON reports from the web page. AFOSI is revising its written operating procedures to comply with this change in operations.

(U//~~FOUO~~) 9. (b)(5)

(b)(5)

(b)(5)

(U//~~FOUO~~) Deputy Secretary of Defense Memorandum dated March 30, 2006, Subject, "Threats to the Department of Defense (DoD)" directs that the TALON Reporting System should be used only to report information regarding possible international terrorist activity. Further, all TALON reports should be retained in accordance with DoDR 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1982.

(b)(5)

(b)(5)



(U//FOUO) The 90 day retention rule in DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons" has been the rule within DoD since the regulation was approved by the Attorney General and the Secretary of Defense in 1982. The 90 day retention rule is not required by Executive Order 12333.

(U//FOUO) (b)(5)



(b)(5)

(U//FOUO) (b)(5)



(b)(5)



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

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).

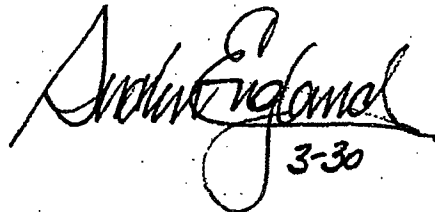
This Memorandum provides interim guidance. Given the importance of capturing threat information in protecting the Department's personnel, property and facilities, I am Directing the Under Secretary of Defense for Intelligence (USD(I)) to convene a working group to examine the integration of threat information 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.



Andrew 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

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.

~~FOR OFFICIAL USE ONLY~~

HRS (UAR)



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

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

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.



Attachment:
As stated

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

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 JTF-CT has full access to the raw, non-validated information. Designated lead Service and Agency components will have access to the TALON database.

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

TALON REPORT GUIDE

~~FOR OFFICIAL USE ONLY~~

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.

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

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

~~FOR OFFICIAL USE ONLY~~

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

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~



Office of the Attorney General
Washington, D. C. 20530

September 23, 2002

MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS

FROM THE ATTORNEY GENERAL *John Ashcroft*

SUBJECT: Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral
Interception Information Identifying United States Persons.

The prevention of terrorist activity is the overriding priority of the Department of Justice and improved information sharing among federal agencies is a critical component of our overall strategy to protect the security of America and the safety of her people.

Section 203 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, 115 Stat. 272, 278-81, authorizes the sharing of foreign intelligence, counterintelligence, and foreign intelligence information obtained through grand jury proceedings and electronic, wire, and oral interception, with relevant Federal officials to assist in the performance of their duties. This authorization greatly enhances the capacity of law enforcement to share information and coordinate activities with other federal officials in our common effort to prevent and disrupt terrorist activities.

At the same time, the law places special restrictions on the handling of intelligence information concerning United States persons ("U.S. person information"). Executive Order 12333, 46 FR 59941 (Dec. 8, 1981) ("EO 12333"), for example, restricts the type of U.S. person information that agencies within the intelligence community may collect, and requires that the collection, retention, and dissemination of such information must conform with procedures established by the head of the agency concerned and approved by the Attorney General. Section 203(c) of the USA PATRIOT Act, likewise, directs the Attorney General to establish procedures for the disclosure of grand jury and electronic, wire, and oral interception information "that identifies a United States person, as that term is defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)."

Pursuant to section 203(c), this memorandum specifies the procedures for labeling information that identifies U.S. persons. Information identifying U.S. persons disseminated pursuant to section 203 must be marked to identify that it contains such identifying information prior to disclosure.

Section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801) provides:

"United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.

Information should be marked as containing U.S. person information if the information identifies any U.S. person. The U.S. person need not be the target or subject of the grand jury investigation or electronic, wire, and oral surveillance; the U.S. person need only be mentioned in the information to be disclosed. However, the U.S. person must be "identified." That is, the grand jury or electronic, wire, and oral interception information must discuss or refer to the U.S. person by name (or nickname or alias), rather than merely including potentially identifying information such as an address or telephone number that requires additional investigation to associate with a particular person.

Determining whether grand jury or electronic, wire, and oral interception information identifies a U.S. person may not always be easy. Grand jury and electronic, wire, and oral interception information standing alone will usually not establish unequivocally that an identified individual or entity is a U.S. person. In most instances, it will be necessary to use the context and circumstances of the information pertaining to the individual in question to determine whether the individual is a U.S. person. If the person is known to be located in the U.S., or if the location is unknown, he or she should be treated as a U.S. person unless the individual is identified as an alien who has not been admitted for permanent residence or circumstances give rise to the reasonable belief that the individual is not a U.S. person. Similarly, if the individual identified is known or believed to be located outside the U.S., he or she should be treated as a non-U.S. person unless the individual is identified as a U.S. person or circumstances give rise to the reasonable belief that the individual is a U.S. person.

Grand jury and electronic, wire, and oral interception information disclosed under section 203 should be received in the recipient agency by an individual who is designated to be a point of contact for such information for that agency. Grand jury and electronic, wire, and oral interception information identifying U.S. persons is subject to section 2.3 of EO 12333 and the procedures of each intelligence agency implementing EO 12333, each of which place important limitations on the types of U.S. person information that may be retained and disseminated by the United States intelligence community. These provisions require that information identifying a U.S. person be deleted from intelligence information except in limited circumstances. An intelligence agency that, pursuant to section 203, receives from the Department of Justice (or

another Federal law enforcement agency) information acquired by electronic, wire, and oral interception techniques should handle such information in accordance with its own procedures implementing EO 12333 that are applicable to information acquired by the agency through such techniques.

In addition, the Justice Department will disclose grand jury and electronic, wire, and oral interception information subject to use restrictions necessary to comply with notice and record keeping requirements and as necessary to protect sensitive law enforcement sources and ongoing criminal investigations. When imposed, use restrictions shall be no more restrictive than necessary to accomplish the desired effect.

These procedures are intended to be simple and minimally burdensome so that information sharing will not be unnecessarily impeded. Nevertheless, where warranted by exigent or unusual circumstances, the procedures may be modified in particular cases by memorandum of the Attorney General, Deputy Attorney General, or their designees, with notification to the Director of Central Intelligence or his designee. These procedures are not intended to and do not create any rights, privileges, or benefits, substantive or procedural, enforceable by any party against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

The guidelines in this memorandum shall be effective immediately

INFORMATION MEMO

FOR: DEPUTY UNDER SECRETARY OF DEFENSE (CI&S)

THROUGH: DIRECTOR, COUNTERINTELLIGENCE, ODUSD (CI&S)

FROM: DAVID A. BURTT, II, DIRECTOR, CIFA

SUBJECT: CIFA Review of Military Department Interim TALON Guidance

- In accordance with the Deputy Secretary of Defense memorandum of March 30, 2006, SUBJECT: Threats to the Department of Defense (DoD), CIFA was required to review the TALON reporting guidance issued by each Department to implement the process established in Enclosure (1) to the memorandum. CIFA is to provide a status report on its review to the Deputy Under Secretary of Defense (Counterintelligence and Security) by May 30, 2006.
- CIFA has reviewed the guidance issued by the "lead components," attached, and finds that all lead components, Army, Navy and Air Force, have drafted instructions for their respective service which comply with the above mentioned memorandum.

My point of contact is (b)(6)

(b)(2)

Attachments:

As stated

Prepared By: (b)(6) Deputy Director, Campaign Management and Integrated Threat Office, (b)(2)



INTELLIGENCE

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

APR 7 2006

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: DoD Integrated Threat Reporting Working Group

As the DoD confronts the threats posed by international and domestic terror groups, foreign intelligence services, and criminal activity, we must examine how we integrate information across the Department and determine if our internal information sharing policies are adequate to face the ever-changing threat environment. The Deputy Secretary of Defense (DEPSECDEF) noted the importance of sharing threat information in his memorandum of March 30, 2006, "Threats to the Department of Defense (DoD)" and thereby directed that I convene a working group to examine this critical area.

Pursuant to the DEPSECDEF's guidance, I have directed the Acting Deputy Under Secretary of Defense for Counterintelligence and Security to convene a working group to examine the interim guidance published by the DEPSECDEF and make recommendations that might improve our policies and procedures for the integration of threat information across the DoD intelligence, counterintelligence (CI), law enforcement, force protection and security communities. The working group should be guided by the need to provide commanders with the most current and actionable information and intelligence possible while providing analysts the ability to connect the dots which indicate a potential threat to the Department. Equally important is ensuring that any proposed policies and procedures protect the rights and civil liberties of our citizens. The working group's findings and recommendations will be reported to me by September 1, 2006.

I request each organization listed in the attachment to this memorandum identify a senior military or civilian (06/GS-15) to participate in the working



group. Your representative should work closely with your organization's CI, force protection, security, intelligence and law enforcement ~~elements~~ and be able to draw upon those communities for their expertise, recommendations, and participation in any sub working groups. The Working Group will have its initial meeting during April 2006.

In order to have an effective and manageable working group, we must limit the number of participating organizations. I recognize that the subject under review will have a Department-wide impact and is of critical interest to all DoD Components. I will share the working group's recommendations with you for comment before providing them to the Deputy Secretary and will keep you informed of the group's progress.

For those organizations on the working group list, please identify your Integrated Threat Reporting Working Group (ITRWG) representative, and provide telephone and e-mail contact information for your ITRWG member to Mr. Michael Donnelly, OUSD(I) CI Directorate, (703) 697-7641 Ext-377; NIPR: Michael.Donnelly@osd.mil. Mr. Donnelly will provide each participant with a read-ahead package and provide a time, date and location for the ITIWG's initial meeting.


Stephen A. Cambone

Attachment:
As stated

TALON WORKING GROUP PARTICIPATING ORGANIZATIONS

Office of the Deputy Under Secretary of Defense (Counterintelligence and Security)

Office of the General Counsel

Department of the Army

Department of the Navy

Department of the Air Force

Joint Chiefs of Staff

United States Northern Command

Defense Intelligence Agency

DoD Inspector General

DoD Counterintelligence Field Activity



INTELLIGENCE

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000
INFO MEMO

FOR: USD(I)

FROM: DUSD (CI&S)

SUBJECT: Integrated Threat Reporting Working Group

- The Integrated Threat Reporting Working Group (ITRWG), mandated by the DEPSECDEF via TAB A, held its first meeting on April 26. A list of participants is at TAB B.

• (b)(5)



- The next ITRWG meeting will be scheduled for the last week of May 2006.

Prepared by: 



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

**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).

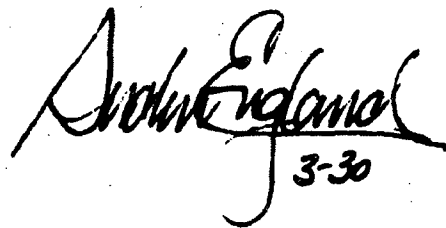
This Memorandum provides interim guidance. Given the importance of capturing threat information in protecting the Department's personnel, property and facilities, I am Directing the Under Secretary of Defense for Intelligence (USD(I)) to convene a working group to examine the integration of threat information 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.



Andrew 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

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.

ITRWG PARTICIPATING ORGANIZATIONS
Participants: primary and backup

Office of the Deputy Under Secretary of Defense (Counterintelligence and Security):

(b)(2), (b)(6)

Office of the General Counsel:

(b)(2), (b)(6)

Department of the Army:

(b)(2), (b)(6)

Department of the Navy:

(b)(2), (b)(6)

Department of the Air Force:

(b)(2), (b)(6)

Joint Chiefs of Staff:

(b)(2), (b)(6)

United States Northern Command:

(b)(2), (b)(6)

Defense Intelligence Agency:

(b)(2), (b)(6)

DoD Inspector General:

(b)(2), (b)(6)

DoD Counterintelligence Field Activity:

(b)(2), (b)(6)



OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INFO MEMO

INTELLIGENCE

FOR: USD(I)

FROM: DUSD(CI&S)

SUBJECT: TALON Question; (b)(5)

(b)(5)

COORDINATION: None

Prepared by:

(b)(6)





INTELLIGENCE

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

ACTION MEMO

FOR: USD (I)

FROM: DUSD (CI&S)

SUBJECT: DoD Integrated Threat Reporting Working Group (ITRWG) TALON Findings

- This memo provides DepSecDef with the findings of the ITRWG (TAB B), convened to examine the integration of threat information across the DoD intelligence, counterintelligence, law enforcement, force protection and security communities, pursuant to the 30 March 2006, memo "Threats to the Department of Defense (DoD)" (TAB C).

(b)(5)



(b)(5)

COORDINATION: See TAB E

Prepared by: (b)(2), (b)(6)



#14



INTELLIGENCE

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

ACTION MEMO

FOR: DEPUTY SECRETARY OF DEFENSE

FROM: UNDER SECRETARY OF DEFENSE (INTELLIGENCE)

SUBJECT: Integrated Threat Reporting Working Group (ITRWG) Recommendations

- This memo responds to your memorandum of March 30, 2006 (TAB C) wherein you directed me to convene a working group to examine the integration of force protection threat information across various DoD communities and provide the results to you.

(b)(5)




(b)(5)



COORDINATION: TAB E

Attachments:
As stated

Prepared by: (b)(2),(b)(6)



TAB A



DEPUTY SECRETARY OF DEFENSE

**1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010**



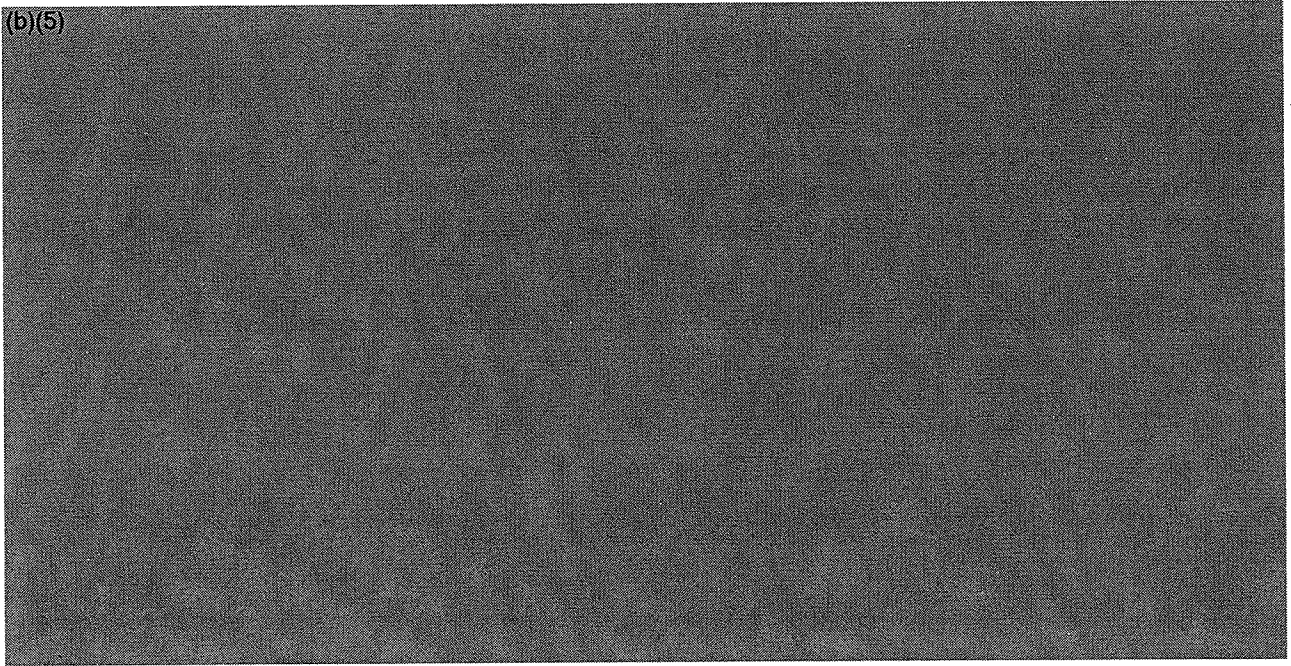
**MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
ASSISTANT TO THE SECRETARY OF
DEFENSE FOR INTELLIGENCE OVERSIGHT
GENERAL COUNSEL OF THE DEPARTMENT
OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF
DEFENSE
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE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

SUBJECT: Reporting Threats to the Department of Defense

(b)(5)



(b)(5)



INTEGRATED THREAT REPORTING WORKING GROUP
RECOMMENDATIONS

(b)(5)



(b)(5)

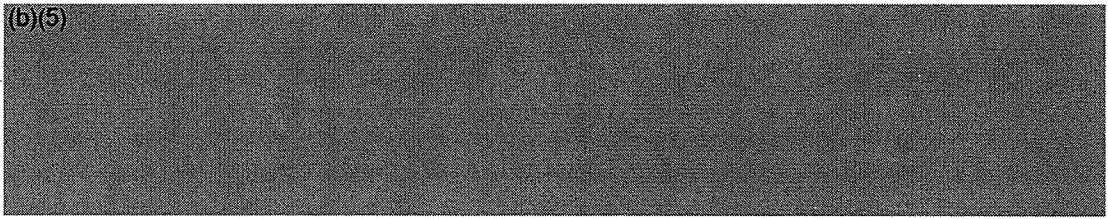


UPDATED TALON REPORTING SYSTEM PROCEDURES

(b)(5)



(b)(5)



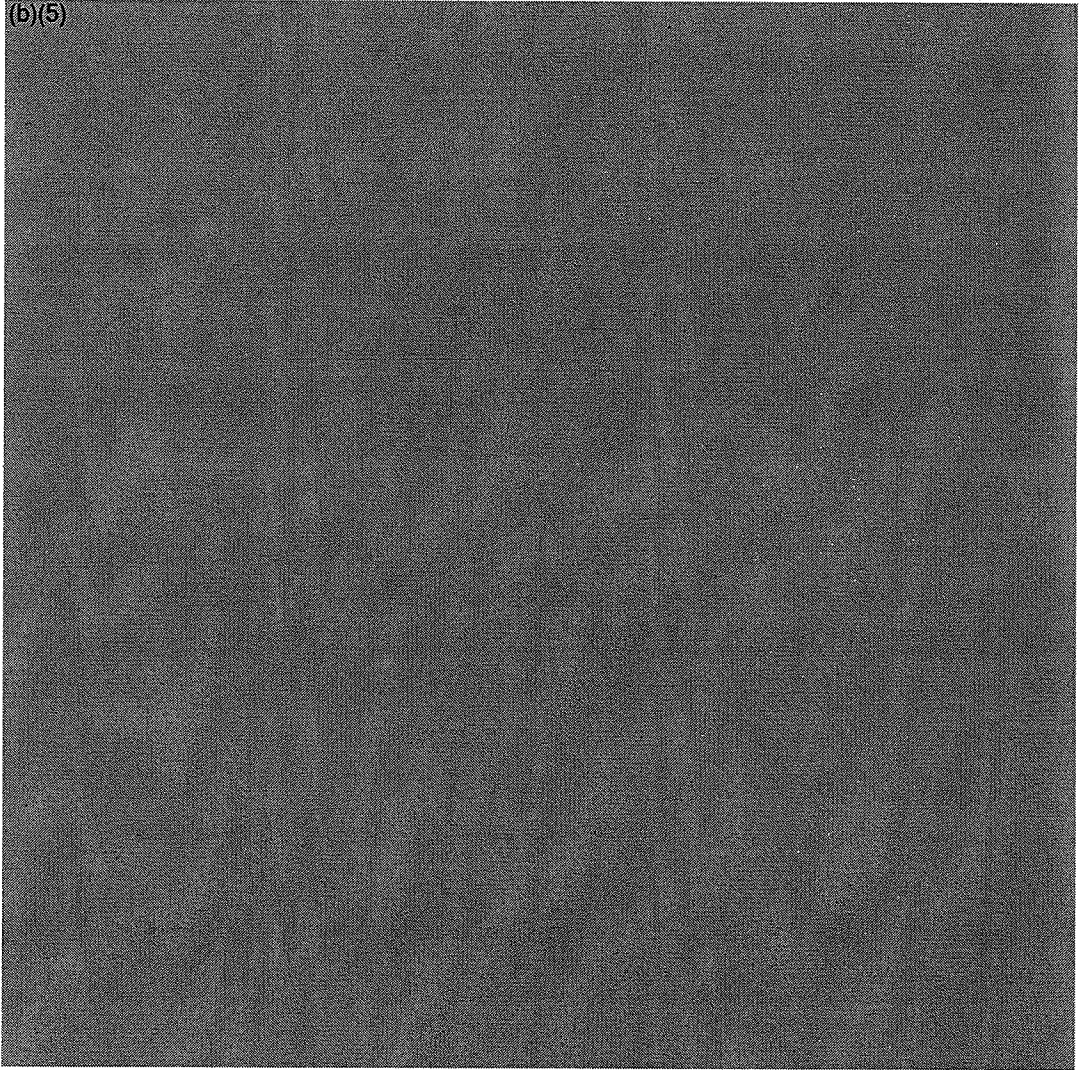
TAB B

INTEGRATED THREAT REPORTING WORKING GROUP
RECOMMENDATIONS

(b)(5)



(b)(5)



TAB C



DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON DC 20301-1010

**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).

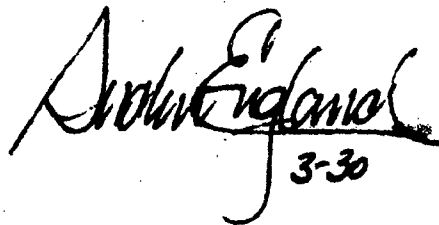
This Memorandum provides interim guidance. Given the importance of capturing threat information in protecting the Department's personnel, property and facilities, I am Directing the Under Secretary of Defense for Intelligence (USD(I)) to convene a working group to examine the integration of threat information 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.



Arthur 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

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.

TAB D



INTELLIGENCE

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

AUG 18 2006


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
DIRECTOR, ADMINISTRATION AND
MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

Subject: DoD Integrated Threat Reporting Working Group Recommendations

In my memorandum of April 07, 2006, "DoD Integrated Threat Reporting Working Group," (ITRWG), I announced the formation of the ITRWG to examine the interim guidance published by the Deputy Secretary in his memorandum of March 30, 2006, "Threats to the Department of Defense (DoD)." The working group was charged with making recommendations that might improve our policies and procedures for the integration of threat information across the DoD intelligence, counterintelligence, law enforcement, force protection, and security communities. I promised to share the working group's recommendations with you for comment before providing them to the Deputy Secretary.

Attached are the working group's recommendations. The Deputy Secretary has requested the working group's finding be presented to him by September 15, 2006. Please provide any comments by September 6, 2006.

Forward your comments or questions to Mr. Michael Donnelly, OUSD (I) CI Directorate, (703) 697-7641 Ext: 377; NIPR: Michael.Donnelly@osd.mil.


Stephen A. Cambone

Attachment:
As stated



INTERGRATED THREAT REPORTING WORKING GROUP RECOMMENDATIONS

1. All initial potential terrorist threat reporting, regardless of the reporting agency, in DoD will be handled as "force protection" information in accordance with DoDD 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003, and routed to a central force protection threat database where it will be available to law enforcement, force protection, and security personnel.
2. The Deputy Secretary of Defense should direct the Joint Staff work with USNORTHCOM through the Joint Capabilities Integration and Development System (JCIDS) process to establish a force protection database which is a program of record and whose capabilities can be used DoD-wide.

COMMENT: USNORTHCOM's Joint Protection Enterprise Network (JPEN) had been serving as the threat reporting database until it was recently shut down due to a lack of funding.

3. The Counterintelligence Field Activity (CIFA), as the program manager for the TALON Reporting System, will review the force protection database and extract data potentially relating to international terrorist activity for analysis. TALON reports, meeting established criteria for TALON reporting, will be created using data extracted from the force protection database. The TALON/Cornerstone database will continue to be maintained pursuant to DoD 5240.1-R, and those organizations with access to the TALON Reporting System will continue to have access to these reports.
4. The Deputy Secretary of Defense should designate a single senior official in the Office of the Secretary of Defense (OSD) to be responsible for DoD force protection and DoD law enforcement policy.

COMMENTS: The Integrated Threat Reporting Working Group (ITRWG) believes the absence of a single OSD lead for law enforcement and force protection has hampered efforts to develop integrated DoD force protection and law enforcement programs and to

effectively address issues impacting those communities within the Department.

- The intelligence, counterintelligence, and security communities are well represented by OUSD (I). However, there is no single entity to champion the other disciplines' equities, seek funding for a single force protection database, deconflict policy issues, etc.
- Law enforcement and force protection equities are spread over numerous OSD organizations.
 - The DoD Inspector General, USD (Personnel & Readiness), ASD (Homeland Defense), ASD (Networks and Information Integration), ASD (Special Operations & Low Intensity Conflict) and DUSD (Counterintelligence & Security), etc., all have law enforcement and force protection equities.
 - The absence of a law enforcement and force protection lead hampers coordination in numerous areas beyond the information sharing equities being addressed by the ITRWG (biometrics, cyber, and legislative affairs for example). The funding of JPEN, IIR tear line considerations, and confusion between intelligence oversight vs Privacy Act issues were specific areas identified during the ITRWG's efforts.

TAB E

COORDINATION
DoD Integrated Threat Working Group (ITRWG) Recommendations to the
Deputy Secretary of Defense

(b)(5)



ITRWG PARTICIPATING ORGANIZATIONS

Participants: primary and backup

Office of the Deputy Under Secretary of Defense (Counterintelligence and Security):

Mr. Mike Donnelly, CI Directorate
(b)(6), Security Directorate

Office of the General Counsel:

(b)(6)

Department of the Army:

(b)(6), USA G2

Department of the Navy:

(b)(6)

Department of the Air Force:

(b)(6)

Joint Chiefs of Staff:

(b)(6)

United States Northern Command:

(b)(6)

Defense Intelligence Agency:

(b)(6)

DoD Inspector General:

(b)(6)

DoD Counterintelligence Field Activity:

(b)(6)

UPDATED TALON REPORTING SYSTEM PROCEDURES

- The Acting Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD(IO)) conducted a review of the DoD TALON Reporting System and made several recommendations which will be adopted. These findings *modify* existing interim TALON Reporting System policy as set forth in the Deputy Secretary of Defense memorandum of March 30, 2006, "*Threats to the Department of Defense (DoD)*." That interim policy, with the below described modifications, will remain in effect until the Assistant Secretary of Defense (Homeland Defense) develops and implements Department-wide procedures for the documentation, storage and exchange of force protection threat information.
- Interim TALON Reporting Policy is modified as follows:
 - The TALON Reporting System's policies apply worldwide, not simply within the United States.
 - Permanent TALON Reporting System Policy, when issued, will explicitly supersede all previous TALON policy.
 - The Counter Intelligence Field Activity (CIFA) is designated as the Executive Agent for the TALON Reporting System.
 - The CIFA will work with the Assistant Secretary of Defense (Homeland Defense) as force protection threat reporting guidance is developed to ensure the force protection data is submitted in a common electronically searchable format which CIFA can use to produce TALONS.
 - Develop protocols between CIFA and the Executive Agent for the proposed DoD-wide force protection database that allow intelligence analysts to view all force protection information held in the database.
 - Insure the next generation of TALON database software contains intelligence oversight (IO) tools required to strengthen system safeguards.
 - Through data analysis CIFA should validate the need for modification to the "90 day" retention rule found in DoD 10 policy.



**DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010**

OCT 12 2006

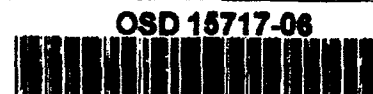
**MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARY OF DEFENSE FOR POLICY
UNDER SECRETARY OF DEFENSE FOR PERSONNEL
AND READINESS
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
GENERAL COUNSEL OF THE DEPARTMENT OF
DEFENSE
INSPECTOR GENERAL OF THE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

SUBJECT: DoD Integrated Threat Reporting Working Group

The Integrated Threat Reporting Working Group (ITRWG) convened by the Under Secretary of Defense for Intelligence (USD(I)) pursuant to the memorandum of March 30, 2006, "Threats to the Department of Defense (DoD)" has submitted its recommendations.

Accordingly, the Assistant Secretary of Defense (Homeland Defense) (ASD(HD)) is designated as the senior OSD principal staff assistant (PSA) for force protection threat reporting. The ASD(HD) will develop Department-wide guidance for the documentation, storage and exchange of force protection threat information related to the protection of DoD personnel, facilities, and forces in transit. The ASD(HD) will establish a DoD-wide force protection threat information database and will provide a status update by December 15, 2006. Until the database is operational and guidance is published, DoD components will use current threat information reporting procedures.

The ITRWG recommends a PSA lead for law enforcement policy. Law enforcement investigative policy will remain under the cognizance of the DoD Inspector General. The USD(I) will convene a working group comprised of the Department's organizations with law enforcement equities. The USD(I) will provide a status on this initiative by December 15, 2006.

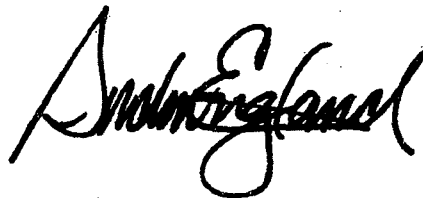


OSD 15717-06

10/12/2006 3:57:35 PM

#15

Attached are several modifications to the interim TALON Reporting System policy of March 30, 2006. The modifications were based upon recommendations by the Acting Assistant to the Secretary of Defense (Intelligence Oversight) and have been implemented where feasible. The USD(I) will incorporate the remaining recommendations once the force protection threat information database has been fully populated and is operational.

A handwritten signature in black ink, appearing to read "Andrew England". The signature is written in a cursive, somewhat stylized font.

Attachment:
Updated TALON Reporting System Procedures

- **The permanent TALON Reporting System policy, written to complement the process that will be developed by ASD(HD), will clarify CIFA's authorities to direct maintenance of TALON Reporting databases regarding IO issues.**



**THE JOINT STAFF
WASHINGTON, DC**

Reply ZIP Code:
20318-0300

DJSM 0868-06
13 September 2006

**MEMORANDUM FOR THE UNDER SECRETARY OF DEFENSE FOR
INTELLIGENCE**

Subject: DOD Integrated Threat Reporting Working Group's Recommendations

1. Thank you for the opportunity to review the subject recommendations.¹ We concur in the overall effort and results of the working group. To enhance understanding across the communities, we are providing clarifying wording for recommendations 1 and 3 in the enclosed matrix.

2. The Joint Staff point of contact is

(b)(6)

(b)(6)

SCOTT S. CUSTER
Major General, USAF
Vice Director Joint Staff

Enclosure

Reference:

- 1 USD(I) memorandum, 18 August 2006, "DoD Integrated Threat Reporting Working Group Recommendations"

cc:
CIDS

