

Inspector General

United States
Department *of* Defense



Report No. 07-INTEL-09
June 27, 2007

The Threat and Local Observation Notice (TALON) Report Program

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 27 JUN 2007		2. REPORT TYPE		3. DATES COVERED 00-00-2007 to 00-00-2007	
4. TITLE AND SUBTITLE The Threat and Local Observation Notice (TALON) Report Program				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Department of Defense Inspector General, 4800 Mark Center Drive, Alexandria, VA, 22350-1500				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 56	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Additional Copies

To obtain additional copies of this report, contact Mr. Sean Mitchell at (703) 604-8815 (DSN) 664-8815 or Mr. Donald A. Ragley at (703) 604-8965.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Office of the Deputy Inspector General for Intelligence at (703) 604-8800 (DSN 664-8800) or fax (703) 604-0045. Ideas and requests can also be mailed to:

Office of the Deputy Inspector General for Intelligence
ODIG-INTEL (ATTN: Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 703)
Arlington, VA 22202-4704

DEPARTMENT OF DEFENSE

hotline

To report fraud, waste, mismanagement, and abuse of authority.

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.osd.mil www.dodig.mil/hotline

Acronyms

CIFA	Counterintelligence Field Activity
FISA	Foreign Intelligence Surveillance Act
JPEN	Joint Protection Enterprise Network
TALON	Threat and Local Observation Notice
UCSC	University of California, Santa Cruz
USD(I)	Under Secretary of Defense for Intelligence
USNORTHCOM	U.S. Northern Command



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

June 27, 2007

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
COMMANDER, U.S. NORTHERN COMMAND
DEPUTY UNDER SECRETARY OF DEFENSE
(COUNTERINTELLIGENCE AND SECURITY)
DIRECTOR, COUNTERINTELLIGENCE FIELD ACTIVITY

SUBJECT: The Threat and Local Observation Notice (TALON) Report Program
(Report No. 07-INTEL-09)

We are providing this report for your information and use. We performed the audit in response to congressional requests. The Counterintelligence Field Activity provided comments. We considered management comments on the draft of this report when preparing the final report. The complete text of the comments is in the Management Comments Section of the report.

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Lois A. Therrien at (703) 604-1613 (DSN 332-1613). See Appendix K for the report distribution. The team members are listed inside the back cover.

A handwritten signature in dark ink, reading "Shelton Young", is positioned above the printed name.

Shelton R. Young
Deputy Inspector General
for Intelligence

Department of Defense Office of Inspector General

Report No. 07-INTEL-09

June 27, 2007

(Project No. D2006-DINT02-0128.000)

The Threat and Local Observation Notice (TALON) Report Program

Executive Summary

Who Should Read This Report and Why? All DoD officials involved in the Threat and Local Observation Notice (TALON) report program and all intelligence, counterintelligence, law enforcement, and force protection personnel should read this report. The report addresses the TALON report program as initially established and as currently implemented.

Background. We performed this audit in response to requests from Congresswomen Zoe Lofgren, on December 30, 2005, and Anna G. Eshoo, on January 12, 2006, on media reporting that DoD had developed and maintains a database for information on U.S. persons conducting domestic anti-war and counter-military protests and demonstrations.

The Air Force Office of Special Investigations developed the TALON report format in 2001 for its Eagle Eye Program, a neighborhood watch program to detect and report suspicious activity of possible targeting of Air Force interests by terrorists. The TALON report program was instituted DoD-wide on May 2, 2003, by Deputy Secretary of Defense memorandum, "Collection, Reporting, and Analysis of Terrorist Threats to DoD Within the United States," because DoD had no formal mechanism to collect and share non-validated domestic threat information between intelligence, counterintelligence, law enforcement, and force protection entities and to analyze that information for indications of foreign terrorist activity. A TALON report consists of raw information reported by concerned citizens and military members about suspicious incidents. The memorandum also directs that TALON reports be provided to the DoD Counterintelligence Field Activity for incorporation into a database repository. The Counterintelligence Field Activity is a designated DoD law enforcement and counterintelligence organization and serves as the bridge between intelligence related to international terrorism information and domestic law enforcement information. In addition, the Commander, U.S. Northern Command's mission is to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within its area of responsibility.

Results. The Counterintelligence Field Activity and the U.S. Northern Command legally gathered and maintained U.S. person information on individuals or organizations involved in domestic protests and demonstrations against DoD.

- TALON reports were generated for law enforcement and force protection purposes as permitted by DoD Directive 5200.27,¹ and not as a result of an

¹ DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense," January 7, 1980.

intelligence collection operation; therefore, no violation of the Foreign Intelligence Surveillance Act occurred.

- The Counterintelligence Field Activity did not comply with the 90 day retention review policy required by DoD Directive 5200.27. We could not determine whether the U.S. Northern Command complied with the policy requirement because all TALON reports were deleted from their database in June 2006 with no archives.
- The Cornerstone database that the Counterintelligence Field Activity used to maintain TALON reports did not have the capability to identify TALON reports with U.S. person information, to identify reports requiring a 90-day retention review, or to allow analysts to edit or delete the TALON reports.

As a result, the Counterintelligence Field Activity maintained TALON reports without determining whether information on organizations and individuals should be retained for law enforcement and force protection purposes.

Distribution of Reports. We reviewed the 1,131 TALON reports that the Counterintelligence Field Activity deleted from the Cornerstone database from December 2, 2005, through January 18, 2006.² The Cornerstone database included about 13,000 TALON reports. Of the 1,131 TALON reports:

- 117 reports originated outside the United States and did not contain information on U.S. persons,
- 263 reports were related to protests and demonstrations, and
- 751 reports did not relate to protests and demonstrations.

Further analysis of the 263 TALON reports for protests and demonstrations showed that:

- 157 reports discussed an action or event that took place, and
- 75 of the 157 reports had criminal actions occur that resulted in arrests, required court appearances, violence, destruction, and required police intervention.

The 75 TALON reports for protests and demonstrations on actions or events with criminal actions demonstrate the value of the TALON reports for law enforcement and force protection purposes.

² As of April 2007, 5,231 TALON reports had been deleted from the Cornerstone database. The reports no longer had any analytical value because they were resolved or they were determined to have no potential terrorism connection, or the reports were on anti-DoD protests. TALON reports were not deleted specifically for containing U.S. person information; instead, the U.S. person information was deleted from the report.

U.S. Person Information and U.S. Persons Identified. We also reviewed the 1,131 TALON reports to identify U.S. person information³ and determined the number of U.S. persons⁴ identified. Of the 1,131 TALON reports:

- 334 reports contained U.S. person information:
 - 142 U.S. persons were identified on 92 protest and demonstration TALON reports, and
 - 429 U.S. persons were identified on 242 TALON reports for other than protests and demonstrations; and
- 797 reports did not contain U.S. person information.

Management Actions. The number of TALON reports being created has dropped significantly since the Deputy Secretary of Defense issued the March 30, 2006, memorandum, “Threats to the Department of Defense.” The memorandum designates that the TALON Reporting System should report information for possible international terrorist activity only and be retained as intelligence information under DoD Regulation 5240.1-R,⁵ rather than law enforcement information.

On October 12, 2006, the Deputy Secretary of Defense issued a memorandum, “DoD Integrated Threat Reporting Working Group,” designating the Assistant Secretary of Defense (Homeland Defense) as the principal staff assistant for reporting force protection threats. The Assistant Secretary was tasked to develop Departmentwide guidance for documenting, storing and exchanging force protection information. The Under Secretary of Defense for Intelligence was tasked to convene a separate working group to discuss law enforcement equities.

In April 2007, the Under Secretary of Defense for Intelligence requested that the Secretary of Defense terminate the TALON program because the results of the last year do not merit continuing the program as currently constituted, particularly in light of its image in the Congress and the media.

As a result of ongoing management actions, we are not making any recommendations.

Management Comments. We provided a draft of this report on May 18, 2007. Although no written response to this report was required, the Counterintelligence Field Activity stated that they anticipate the TALON program will be terminated. However, the report will assist the Assistant Secretary of Defense (Homeland Defense) in crafting an efficient and effective suspicious activity reporting system.

³ Any information that pertains to a U.S. person is U.S. person information; however, if a U.S. person is not identified, the same information is not U.S. person information.

⁴ The types of U.S. persons identified are individuals, organizations, and businesses.

⁵ DoD Regulation 5240.1-R, “Activities of DoD Intelligence Components That Affect United States Persons,” December 1982.

Table of Contents

Executive Summary	i
Background	1
Objectives	3
Finding	
Reports for Protests and Demonstrations and Reports Containing U.S. Person Information	5
Appendixes	
A. Scope and Methodology	15
B. Congressional Request from Congresswoman Zoe Lofgren	17
C. Congressional Request from Congresswoman Anna G. Eshoo	20
D. Response to Congresswoman Lofgren	23
E. Response to Congresswoman Eshoo	29
F. Deputy Secretary of Defense May 2, 2003, Memorandum	30
G. Deputy Secretary of Defense March 30, 2006, Memorandum	32
H. Deputy Secretary of Defense October 12, 2006, Memorandum	34
I. Deputy IG for Intelligence June 20, 2006, Memorandum	38
J. Director, Joint Staff July 24, 2006, Memorandum	40
K. Report Distribution	41
Management Comment	
Counterintelligence Field Activity	43

Background

We performed this audit in response to congressional requests from Congresswomen Zoe Lofgren, on December 30, 2005, and Anna G. Eshoo, on January 12, 2006, on media reports that DoD developed and maintains a database for information on U.S. persons conducting domestic anti-war and counter-military protests and demonstrations.

Threat and Local Observation Notice (TALON) Report. The Air Force Office of Special Investigations developed the TALON report format in 2001 for its Eagle Eye Program, a neighborhood watch program to detect and report suspicious activity of possible targeting of Air Force interests by terrorists. The Air Force Office of Special Investigations definition states that:

The TALON report is a law enforcement report designed to report anomalies, observations that are suspicious against the steady state context, and immediate indicators of potential threats or antiterrorism concerns. TALONs are raw, non-validated information, may or may not be related to an actual threat, and by their very nature, may be fragmented and incomplete.

Deputy Secretary of Defense memorandum, “Collection, Reporting, and Analysis of Terrorist Threats to DoD Within the United States,” May 2, 2003 (Appendix F), instituted the TALON report program DoD-wide. The memorandum states that DoD had no formal mechanism to collect and share nonvalidated domestic threat information between intelligence, counterintelligence, law enforcement, and force protection entities and to analyze that information for indications of foreign terrorist activity. The DoD TALON report was established to capture nonvalidated information on domestic threats, pass that information to analysts, and incorporate it into the DoD process for warning against terrorism. A TALON report is raw information reported by concerned citizens and military members about suspicious incidents. Information in TALON reports is not validated, may or may not relate 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 information on potential threats to DoD personnel, facilities, and resources. The TALON report is not designed to take the place of the formal DoD intelligence reporting process. The framework established by the memorandum specified that the information contained in TALON reports is for commanders at all levels that have force protection responsibilities and for analysts to use in determining the aggregate terrorist threat to DoD people and resources.

The May 2, 2003, Deputy Secretary of Defense memorandum also directed that TALON reports be provided to the DoD Counterintelligence Field Activity (CIFA) for the information to be incorporated into a database. CIFA is to provide access to the full database to the Defense Intelligence Agency, Joint Intelligence Task Force-Combating Terrorism to support its terrorism-warning mission.

Homeland Defense. The U.S. Northern Command (USNORTHCOM) was created October 1, 2002, as a result of the terrorist attacks of September 11, 2001.

The USNORTHCOM mission is to conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests within its area of responsibility.

DoD Directive 2000.12, "DoD Antiterrorism (AT) Program," August 18, 2003 (current as of November 21, 2003), assigns the Commander, USNORTHCOM the authority to execute force protection responsibilities and the antiterrorism program through which it will integrate those responsibilities. The directive also provides several definitions.

- **Domestic Terrorism.** Terrorism perpetrated by the citizens of one country against persons in that country. Domestic terrorism also includes acts against citizens of a second country when they are in the host country and not the principal or intended target.
- **Force Protection.** Actions taken to prevent or mitigate hostile actions against DoD personnel (including family members), resources, facilities, and critical information.
- **Physical Security.** That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.
- **Security Organizations.** Military law enforcement, military criminal investigative organizations, and DoD-contracted security personnel.
- **Terrorism.** The calculated use of unlawful violence or threat of unlawful violence to inculcate fear and to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

The USNORTHCOM used TALON reports to assist the force protection mission. TALON reports were maintained in the USNORTHCOM Joint Protection Enterprise Network (JPEN).

CIFA. DoD Directive 5105.67, "Department of Defense Counterintelligence Field Activity (DoD CIFA)," February 19, 2002, establishes CIFA as a field organization of the Under Secretary of Defense for Intelligence (USD[I]) whose mission is to develop and manage DoD counterintelligence programs and functions that protect DoD. Those programs include counterintelligence support to protect DoD personnel, resources, critical information, research and development programs, technology, critical infrastructure, economic security, and U.S. interests against foreign influence and manipulation, as well as to detect and neutralize espionage against DoD. CIFA is funded as part of the National Intelligence Program, but it is to carry out its assigned function and responsibilities by operating as a law enforcement organization under the authorities vested in the Secretary of Defense in title 10, United States Code.

However, the law enforcement responsibilities do not replace or supersede those responsibilities assigned to the DoD criminal investigative organizations.⁶

DoD Directive 2000.12 states that the following are two of the CIFA antiterrorism responsibilities.

- Establish a threat analysis capability designed to collect, fuse, and analyze domestic law enforcement information with foreign intelligence and counterintelligence information in support of the DoD combating terrorism mission. CIFA, as a designated DoD law enforcement and counterintelligence organization, is to support the efforts of the Joint Intelligence Task Force for Combating Terrorism by serving as the bridge between intelligence related to international terrorism and domestic law enforcement information.
- Maintain a domestic law enforcement database that includes information related to potential terrorist threats directed against DoD.

NBC News Report. On December 13, 2005, NBC News aired a report, “Is the Pentagon spying on Americans?” NBC reported that a secret Pentagon database obtained by NBC News tracks “suspicious” domestic groups, and a secret 400-page DoD document lists more than 1,500 “suspicious incidents” across the country over a recent 10-month period. A small group of activists planning a protest of military recruiting at local high schools in Lake Worth, Florida, was listed as a “threat.”

Congressional Requests. In a December 30, 2005, letter to the DoD Inspector General, Congresswoman Zoe Lofgren requested an investigation of recent allegations that the DoD had developed and maintains a database of information on U.S. persons, apparently collected in violation of DoD regulations and the Foreign Intelligence Surveillance Act (FISA). Congresswoman Lofgren’s letter specifically referenced the NBC News report. The letter included seven questions about the TALON reporting program and the authority to report and maintain the information; specifically, information about domestic anti-war or counter-military recruitment groups (protests and demonstrations). See Appendix B for the request from Congresswoman Lofgren and Appendix D for our response.

Subsequently, in a January 12, 2006, letter to the DoD Inspector General, Congresswoman Anna G. Eshoo requested a review of the DoD activities at the University of California, Santa Cruz (UCSC). See Appendix C for the request from Congresswoman Eshoo and Appendix E for our response.

⁶ The Defense Criminal Investigative Service, the Army Criminal Investigation Command, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations are the defense criminal investigative organizations.

Objectives

We performed the audit in response to congressional requests. Our overall objective was to examine “allegations that the Department of Defense (DoD) has developed and maintains a database of information on U.S. persons, apparently collected in violation of DoD regulations and the Foreign Intelligence Surveillance Act (FISA).” We focused our efforts on TALON reports related to protests and demonstrations. See Appendix A for a discussion of the scope and methodology and prior coverage.

We found no evidence that FISA applied to the TALON reporting process. Further discussion is included in Appendix D.

Reports for Protests and Demonstrations and Reports Containing U.S. Person Information

CIFA and USNORTHCOM legally gathered and maintained information on organizations and individuals, including U.S. citizens, involved in domestic demonstrations against DoD. We found no evidence that the effort was the result of an intelligence collection operation. Rather, the TALON reports on protests and demonstrations were generated for law enforcement and force protection purposes, which is permitted under DoD Directive 5200.27.

While CIFA did not violate the law in getting or maintaining information related to demonstrations, it did not follow the information retention criteria in DoD Directive 5200.27, which require such information to be destroyed within 90 days unless retention is required by law or specifically authorized under criteria established by the Secretary of Defense. We could not determine whether USNORTHCOM complied with the DoD 90-day retention review policy because all TALON reports were deleted from JPEN on November 30, 2005, without being archived, and the system was turned off in June 2006.

CIFA retains TALON reports on its Cornerstone database. The Cornerstone database initially could not identify TALON reports with U.S. person information, identify reports requiring a 90-day review, or allow analysts to edit or delete the TALON report. Only CIFA information technology personnel had the ability to delete TALON reports. As a result, CIFA maintained TALON reports without determining whether information on organizations and individuals should be retained for law enforcement and force protection purposes.

Our detailed review of 1,131 TALON reports removed from the CIFA database showed that 263 reports pertained to protests and demonstrations. Of the 263 reports, 157 reports discussed actual actions or events that occurred. Further, 75 of the 157 reports on actual actions or events resulted in reported arrests, required court appearances, violence, destruction, and police intervention. The 75 TALON reports demonstrate that they are necessary to inform local commanders of protests and demonstrations planned for their vicinity for law enforcement and force protection purposes, and not as intelligence information.

Criteria for Gathering and Retaining Information on U.S. Persons

The TALON reports were generated for law enforcement and force protection purposes. We found no evidence that the U.S. person information for organizations and individuals that were not affiliated with the DoD resulted from

an intelligence collection operation. Therefore, the TALON reports were maintained as law enforcement information and were subject to DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense," January 7, 1980.

DoD Gathering U.S. Person Information for Law Enforcement and Force Protection Purposes. DoD Directive 5200.27 establishes general policy for collecting, processing, storing, and disseminating information on persons not affiliated with DoD. DoD Components are authorized to gather information that is essential for protecting DoD functions and property, personnel security, and operations related to civil disturbance. It specifies that nothing in the directive should be interpreted as prohibiting prompt reporting to law enforcement agencies of any information that might threaten life or property, or violate law, or prohibit keeping a record of such a report. The directive specifically prohibits:

- gathering U.S. person information on organizations or individuals not affiliated with the DoD beyond that which is essential to accomplish assigned DoD missions;
- gathering information on U.S. persons solely because they oppose Government policy;
- covert or deceptive surveillance or penetration of civilian organizations unless specifically authorized; and
- assigning DoD personnel to attend public or private meetings, demonstrations, or other similar activities for the purpose of gathering information.

DoD Gathering U.S. Person Information for Intelligence Purposes. DoD Regulation 5240.1-R, "Activities of DoD Intelligence Components That Affect United States Persons," December 1982, applies only to DoD intelligence components and does not apply to law enforcement activities that may be undertaken by the DoD intelligence components. However, when a DoD intelligence component's investigation or inquiry establishes reasonable belief that a crime has been committed, the intelligence component refers the matter to the appropriate law enforcement agency or, if the intelligence component is authorized to conduct law enforcement activities, it continues the investigation under appropriate law enforcement procedures. The regulation specifies that information that identifies a U.S. person may be collected if it is necessary to conduct a function assigned to the collecting component, and if the information falls under the 13 categories. The following four categories are pertinent to TALON reports.

- Information Obtained With Consent,
- Publicly Available Information,
- Physical Security, or
- Administrative Purposes.

DoD Retention of U.S. Person Information. DoD Directive 5200.27 requires U.S. person information for organizations and individuals not affiliated with the DoD to be destroyed within 90 days, unless retention is required by law or specifically authorized under criteria established by the Secretary of Defense. DoD Regulation 5240.1-R also contains a 90-day temporary retention clause for determining whether the information may be permanently retained.

TALON Reporting and Retention

On May 2, 2003, the Deputy Secretary of Defense memorandum established the TALON reporting program to document and immediately disseminate potential threat information to DoD personnel, facilities, and resources. The memorandum directed that CIFA and designated “lead Components” in the Services, combatant commands, and Defense agencies are authorized to retain TALON information as necessary to conduct their analysis mission. A law enforcement database was needed to maintain this information, whether required by law or authorized under criteria established by the Secretary of Defense or his designee.

TALON Reporting. We found no evidence to suggest that the TALON reports were generated as a result of intelligence activities; rather, the TALON reports were generated for law enforcement and force protection purposes, as permitted under DoD Directive 5200.27. Specifically, the TALON reports were developed from information provided to the security and law enforcement personnel at military facilities and/or intelligence personnel. The information was from concerned individuals such as citizens; military personnel, performing their official duties and as citizens; and law enforcement personnel. People are concerned when they hear, see, or are informed about suspicious incidents being planned, that happen at a military facility, or that involve military personnel, such as an incident at a recruiting fair.

TALON Retention. TALON reports were primarily maintained on two databases, one managed by CIFA and one managed by USNORTHCOM.

CIFA. CIFA retains TALON reports on its Cornerstone database. The Cornerstone database was originally created to track foreign visitors to DoD facilities, and it had limited analytical capabilities. The Services and other organizations produce the TALON reports which are integrated into the Cornerstone database, either manually (Army and Navy) or with an automation tool (Air Force). Other agencies create their TALON reports directly in the Cornerstone database.

CIFA did not comply with the retention requirements of DoD Directive 5000.27, which require CIFA to review information on U.S. persons within 90 days. Prior to December 2005, CIFA did not destroy any TALON reports or delete any U.S. person information, including those TALON reports on protests and demonstrations. The Cornerstone database could not identify reports with U.S. person information, identify reports requiring a 90-day review, or allow analysts to edit or delete the TALON reports because the original requirements for the Cornerstone TALON application code were not developed with oversight

requirements in mind. Only CIFA information technology personnel had the ability to delete TALON reports. As a result, CIFA maintained TALON reports without determining whether information on organizations and individuals should be retained for law enforcement and force protection purposes.

USNORTHCOM. Under DoD Directive 2000.12, the Commander, USNORTHCOM was given the authority to execute force protection responsibilities and the antiterrorism program. In June 2004, the Commander, USNORTHCOM selected JPEN as the database for reporting suspicious activity and as the primary database within USNORTHCOM for retaining TALON reports.

Because all TALON reports from the NORTHCOM JPEN were deleted in November 2005 and the system was terminated in June 2006, we could not determine USNORTHCOM compliance with the 90-day requirement that U.S. person information be destroyed unless its retention is required by law or authorized by the Secretary of Defense. Appendices I and J show that the JPEN system was terminated due to the lack of funding when the system was transferred from the Joint Staff to USNORTHCOM.

Retention Legality. CIFA was legally allowed to possess and retain information on U.S. persons. The information was obtained and used for legitimate law enforcement purposes. Law enforcement purposes included force protection of DoD personnel, equipment, and facilities. We determined that the information was not collected for intelligence or counterintelligence purposes. CIFA did not use the information in an attempt to monitor First Amendment activities of U.S. persons. We did determine that, during the early stages of the TALON program, CIFA was not reviewing the U.S. person information as part of a 90-day review requirement cited in DoD Directive 5200.27. However, failure to conduct the 90-day review was not illegal; it was a regulatory violation. CIFA was not intentionally engaged in any illegal, unauthorized, or restricted activity to monitor the lawful actions of U.S. persons. CIFA has since put systems in place to conduct 90-day reviews in every case.

DoD Review of the TALON Reports

As a result of the concerns raised by the NBC News reports and other media reporting, the Deputy Secretary of Defense issued a memorandum, "Retention and Use of Information for the TALON System," January 13, 2006, which directed that the Director, CIFA advise the USD(I) by January 17, 2006, that all reports in the TALON database had been reviewed, and that any reports, which should not be in the database, had been identified. The USD(I) chartered a working group to review and recommend changes to policy and procedures employed in the TALON program to comply with DoD policy.

CIFA Oversight Review. The review of the CIFA Cornerstone database was manpower intensive, since, as previously discussed, there were limited review capabilities inherent in the system. From December 2, 2005, through January 18,

2006, CIFA deleted 1,131 TALON reports⁷ from the Cornerstone database. New controls were implemented requiring review of TALON reports before entering them into the Cornerstone database.⁸ For existing TALON reports in Cornerstone, CIFA made various updates to the Cornerstone system, including Version 4.3, released in April 2006. Version 4.3 provides a select group of designated CIFA analysts with the ability to edit U.S. person information located anywhere in the TALON report; it also provides a 90-day alert flag for TALON reports requiring future review and a tracking mechanism for U.S. person edits. As a result, the designated CIFA analysts have deleted or edited U.S. person information.

Report Purpose. The purpose of the TALON reports has changed. The TALON report program was established in May 2003 for intelligence, counterintelligence, law enforcement and force protection entities to record suspicious activities. A law enforcement database was required to maintain this information. However, on February 2, 2006, the USD (I) issued a memorandum which changed this requirement and designated the Cornerstone database as a counterintelligence database. The memorandum states that CIFA will maintain all TALON reports within the Cornerstone database, or elsewhere in CIFA, under procedures as specified for intelligence components in DoD Regulation 5240.1-R. Further, on March 30, 2006, the Deputy Secretary of Defense issued a memorandum, “Threats to the Department of Defense,” which states that DoD completed its TALON review and determined that the TALON system should be used only to report possible international terrorist activity, and that all TALON reports should be retained in accordance with DoD Regulation 5240.1-R. The memorandum also provided interim guidance (Appendix G).

Intelligence Oversight Review of the TALON Reporting System

In the wake of concerns about the TALON reporting system, the Assistant to the Secretary of Defense for Intelligence Oversight conducted a review and issued a report, “Intelligence Oversight Review of the TALON Reporting System,” May 25, 2006. The report states that no single office has the authority to direct the Services and other reporting agencies in program execution and recommends that an Executive Agent be designated with the authority to issue regulations and prescribe procedures for the TALON reporting system. The report also states that there was confusion over which regulations applied to retaining information in the Cornerstone database. The March 30, 2006, Deputy Secretary of Defense memorandum provided clear direction for the DoD Intelligence Community by directing that the TALON reporting system should be used to report information

⁷ As of April 2007, 5,231 TALON reports had been deleted from the Cornerstone database. The reports no longer had any analytical value because they were resolved or they were determined to have no potential terrorism connection, or the reports were on anti-DoD protests. TALON reports were not deleted specifically for containing U.S. person information; instead, the U.S. person information was deleted from the report.

⁸ As of April 2007, CIFA had rejected 607 entries into the Cornerstone database as TALON reports.

on possible international terrorist activity only, and that all TALON reports should be retained in accordance with DoD Regulation 5240.1-R.

On October 12, 2006, the Deputy Secretary of Defense issued a memorandum, "DoD Integrated Threat Reporting Working Group," that modifies the interim policy on the TALON Reporting System, March 30, 2006, based on the recommendations of the Acting Assistant to the Secretary of Defense for Intelligence Oversight. The memorandum designates CIFA as the Executive Agent for the TALON Reporting System (Appendix H.)

TALON Reports for Protests and Demonstrations

From December 2, 2005, through January 18, 2006, CIFA deleted 1,131 TALON reports that did not meet the suspected international terrorist activity or the DoD Regulation 5240.1-R retention requirements. The deleted reports pertained to criminal activity such as Be On the Look Out (BOLO) reports; resolved activity with no DoD threat or foreign terrorist link, such as innocent photography by tourists or private citizens; bomb threats; and other activity not related to potential international terrorists.

Some of the TALON reports deleted from the Cornerstone database were related to domestic anti-war or counter-military recruitment groups' protests and demonstrations. The TALON reports were manually reviewed by both CIFA and DoD IG personnel. CIFA identified TALON reports that referenced "protest" and "demonstration." Our review also included TALON reports that discussed vandalism, destruction, theft, and/or violence against a recruitment center or a recruiter as protests and demonstrations.

The deleted TALON reports for this audit and other reviews were converted into text documents and are maintained on compact disks controlled by the CIFA General Counsel.

CIFA Results. CIFA identified 186 of the 1,131 TALON reports as protests and demonstrations and 945 that did not relate to protests and demonstrations.

DoD IG Results. We reviewed the 1,131 TALON reports that CIFA deleted from the Cornerstone database and identified 263 reports related to protests and demonstrations and 868 reports that did not. Because 117 of the 868 reports were from outside the United States and did not contain U.S. person information, 751 TALON reports originating in the United States do not relate to protests and demonstrations.

Analysis of the 263 TALON reports on protests and demonstrations showed that 157 of the reports identified an action or event that took place. Of the 157 TALON reports, 75 had criminal actions occur that resulted in arrests, required court appearances, violence, destruction, and required police intervention. Given that about half of the protest and demonstration events had criminal actions occur, creating TALON reports to inform local commanders of protests and demonstrations planned for their vicinity appears to be justified and

reinforces the reason why those reports were created for force protection and law enforcement purposes and not as intelligence information.

DoD IG Review of TALON Reports for U.S. Person Information and for U.S. Persons Identified

We reviewed the 1,131 TALON reports for U.S. person information and to determine how many U.S. persons were identified. Any information that pertains to a U.S. person is U.S. person information; however, if a U.S. person is not identified, the same information is not U.S. person information. Therefore, all potential U.S. person information must be reviewed and a U.S. person identified before the final decision can be made as to what is U.S. person information in each report.

Definition. A U.S. person is defined in section 1801 (i), title 50, United States Code (50 U.S.C. 1801(i)), as a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association in which a substantial number of members 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.

Identification of U.S. Persons. During the CIFA review of the TALON reports to identify U.S. person information, officials debated what information specifically identified a U.S. person. Although CIFA ultimately decided upon a stringent interpretation during its review of TALON reports, the officials changed what information identifies a U.S. person. CIFA decided that any potential U.S. person information would be identified as U.S. person information, whether the subject of a TALON, a location, a point of reference, the source who provided the information, or military and law enforcement personnel.

During our review of the TALON reports, we did not use the CIFA definition to identify U.S. persons. We primarily designed our definition to provide an accurate response to the intent of the congressional questions. The DoD IG did not include U.S. person information in the TALON reports that identify ancillary personnel. For example, we did not include the people who provided or handled the information, most of whom were Government employees, or consider data related to victims, sources of information, witnesses and report creators as U.S. person information.

For example, if a TALON report stated:

John Doe witnessed a man throw an object at the DoD IG building, then jump into a blue Chevy sedan and speed away down Army Navy Drive. The Chevy turned left just past the Embassy Suites.⁹

⁹ This example was created to demonstrate the difference between the determinations made by CIFA and the DoD IG. This is not a real TALON report.

The CIFA review would have identified this report as containing U.S. person information, resulting from John Doe, Chevy, and/or Embassy Suites. We would have determined there was no U.S. person information because John Doe was the witness who reported the incident so the information was obtained with consent, Chevy was the type of car and not a company we are interested in, and Embassy Suites is just a point of reference and not a business being identified.

Application. Many CIFA personnel reviewed the 1,131 TALON reports from September 2005 through January 2006.¹⁰ As a result, the determination of TALON reports that contained U.S. person information was not consistent. During our review, one auditor analyzed all 1,131 TALON reports and did not determine U.S. person information until the last step to ensure consistency.

Results. CIFA identified 186 TALON reports on protests and demonstrations, with 82 of the reports containing U.S. person information. CIFA did not identify the type or quantity of U.S. persons identified in the 82 TALON reports because of time constraints and the labor intensive nature of the review. CIFA only tracked “yes” or “no” for U.S. person information in the TALON report.

DoD Directive 5200.27 discusses U.S. person information for organizations and individuals not affiliated with the DoD, therefore, we did not include military personnel. However, we did not exclude DoD civilian or DoD contractor employees or DoD contractors. As a result, some of the individuals and businesses identified may actually be exempt because of their DoD affiliation, in which case, these numbers may be overstated. We reviewed all potential U.S. person information and categorized the number of U.S. persons identified in the 1,131 TALON reports into individuals, organizations, and businesses.

U.S. Person Information. Table 1 shows that we identified 263 TALON reports on protests and demonstrations, with 92 of these reports containing U.S. person information. The 117 reports that originated outside of the United States did not have U.S. person information. We also identified an additional 242 TALON reports that contained U.S. person information. In total, we identified 334 TALON reports that identified U.S. persons.

U.S. Persons. As shown in Table 2, DoD reported and maintained information on 571 U.S. persons in 334 TALON reports. There are 142 U.S. persons identified in the 92 “protest and demonstration” TALON reports and 429 U.S. persons identified in the “other” 242 TALON reports. The U.S. person information included subjects; sources; witnesses; victims; interviewees; illegal

¹⁰ The CIFA personnel began their review in September 2005; TALON reports were deleted from Cornerstone from December 2, 2005, through January 18, 2006.

Table 1. TALON Reports Containing U.S. Person Information Deleted From December 2, 2005, through January 18, 2006

	<u>Yes</u>	<u>No</u>	<u>Total</u>
Protests and demonstrations	92	171	263
Not protest or demonstration	242	509	751
Not in the United States		117	117
Total	334	797	1,131

aliens; famous people referenced for quotes, positions and scheduled appearances; law enforcement officials involved; and the agent creating the TALON. Therefore, we did not identify as U.S. person information:

- the sources, because they provided the information;
- victims or witnesses, if they were the source;
- famous people referenced for quotes, positions, and scheduled appearances because they weren't included as themselves; or
- law enforcement officials doing their job.

Table 2 shows the number of U.S. persons identified by category.

Table 2. U.S. Persons Identified in the 334 TALON Reports

	<u>Protests and Demonstrations (92 Reports)</u>	<u>Others (242 Reports)</u>	<u>Total</u>
Individuals	38	342	380
Organizations	104	6	110
Company or business		81	81
Total	142	429	571

Current TALON Reporting

Since the March 30, 2006, Deputy Secretary of Defense memorandum, “Threats to the Department of Defense,” was issued, TALON reports are reporting possible international terrorist activity only and are being retained in accordance with DoD Regulation 5240.1-R. The average number of TALON reports generated has dropped from 49 to 7 per month. As previously stated, CIFA stringently reviews a TALON report before it is entered into the Cornerstone database, which resulted in 607 reports being rejected as of April 2007.

The TALON reports were initially used to document and immediately disseminate potential threat information to DoD personnel, facilities, and resources for commanders at all levels that have force protection responsibilities. There is still a need for law enforcement and force protection information to be generated and disseminated.

Recognizing this need, on October 12, 2006, the Deputy Secretary of Defense issued a memorandum, “DoD Integrated Threat Reporting Working Group,” designating the Assistant Secretary of Defense (Homeland Defense) as the principal staff assistant for reporting threats to force protection. The Assistant Secretary was tasked to develop Department-wide guidance for documenting, storing, and exchanging force protection information. The Under Secretary of Defense for Intelligence was tasked to convene a separate working group to discuss law enforcement equities (Appendix H.)

In April 2007, the Under Secretary of Defense for Intelligence requested that the Secretary of Defense terminate the TALON program because the results of the last year did not merit continuing the program as currently constituted, particularly in light of its image in the Congress and the media.

As a result of the ongoing management actions, this report does not include any recommendations.

Appendix A. Scope and Methodology

We performed this audit in response to congressional requests on December 30, 2005, and January 12, 2006. We reviewed the Cornerstone database, TALON reports, the TALON report process, the JPEN report process, the pertinent laws and regulations, and answered the seven questions from Congresswoman Lofgren and the question from Congresswoman Eshoo.

We visited, contacted, or conducted interviews with officials from the Office of the Deputy Under Secretary of Defense for Counterintelligence and Security, CIFA, USNORTHCOM, and the generating organizations.

We reviewed all 1,131 TALON reports deleted by CIFA from December 2, 2005, through January 18, 2006. The reports were removed from the Cornerstone database and saved as text documents for this audit and other required reviews. The CIFA General Counsel maintains control of the compact disks.

Each of the 1,131 TALON reports was opened and reviewed, and pertinent information was copied to a spreadsheet for standardization that allowed analysis. The 117 TALON reports discussed events that did not occur in the United States and did not contain U.S. person information, so no further analysis was performed. The remaining 1,014 TALON reports were separated into protests and demonstrations (263 TALON reports) and other (751 TALON reports). Each of the 263 TALON reports on protests and demonstrations were categorized as an event that took place, that was being planned, or as potential events or “how to” information; 157 were events that took place. We identified 75 of the 157 TALON reports on protest and demonstration events that took place that made arrests, required court appearances, were violent or destructive, or required police intervention. After agreeing with the DoD IG General Counsel on what information identified a U.S. person, the TALON reports containing U.S. person information were identified and the number of U.S. persons identified was calculated by type of information.

We performed this audit from February 2006 through May 2007 in accordance with generally accepted government auditing standards.

Scope Limitations. We limited most of our review to the 1,131 TALON reports that CIFA deleted from the Cornerstone database from December 2, 2005, through January 18, 2006. Given the changes implemented as a result of the Deputy Secretary of Defense memorandum and the resulting decrease in TALON reporting, we believe that these deleted TALON reports had the highest risk of noncompliance with laws or regulations.

Because 334 of the 1,131 TALON reports contain U.S. person information, we did not make copies. Our audit working papers do not have any TALON reports. Our analysis of the TALON reports is recorded on spreadsheets, with U.S. person information deleted. The specific data contained in the spreadsheets can be verified to the TALON report data by the TALON report number.

The USNORTHCOM JPEN deleted all TALON reports in November 2005 and terminated JPEN in June 2006. This system did not have the capability to archive records so all of the information was lost. Therefore, we could not compare the information in JPEN to the 1,131 TALON reports.

The scope of the audit was also limited in that we did not review management controls.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit. The TALON reports reviewed had been removed from the Cornerstone database and were saved as text documents or paper copies. The number of monthly TALON reports received was calculated by counting the number of reports with a report date in each month.

Government Accountability Office High-Risk Area. The Government Accountability Office identified several high-risk areas in DoD. This report provides coverage of the Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security high-risk area.

Prior Coverage. During the last 4 years, the Assistant to the Secretary of Defense for Intelligence Oversight issued one report related to TALON reports.

Assistant to the Secretary of Defense for Intelligence Oversight Report,
“Intelligence Oversight Review of the TALON Reporting System,” May 25, 2006

Appendix B. Congressional Request from Congresswoman Zoe Lofgren

ZOE LOFGREN
16TH DISTRICT, CALIFORNIA

• COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON COURTS, THE INTERNET,
AND INTELLECTUAL PROPERTY
SUBCOMMITTEE ON IMMIGRATION,
BORDER SECURITY, AND CLAIMS

• COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEE ON INTELLIGENCE, INFORMATION
SHARING, AND TERRORISM
RISK ASSESSMENT, RANKING MEMBER
SUBCOMMITTEE ON ECONOMIC SECURITY,
INFRASTRUCTURE PROTECTION, AND CYBERSECURITY
SUBCOMMITTEE ON MANAGEMENT, INTEGRATION,
AND OVERSIGHT

• COMMITTEE ON HOUSE ADMINISTRATION

Congress of the United States
House of Representatives
Washington, DC 20515-0516

PLEASE RESPOND TO:

☐ 102 CAMDEN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3072
(202) 225-3336 (FAX)

☐ 635 NORTH FIRST STREET
SUITE B
SAN JOSE, CA 95112
(408) 271-8700
(408) 271-8713 (FAX)

☐ zoe.lofgren@mail.house.gov
www.house.gov/lofgren

December 30, 2005

Mr. Thomas F. Gimble
Acting Inspector General
U.S. Department of Defense
c/o Office of Communications and Congressional Liaison
400 Army Navy Drive
Arlington, VA 22202-4704

Dear Mr. Gimble:

I write to ask that you begin an immediate investigation of recent allegations that the Department of Defense (DOD) has developed and maintains a database of information on United States persons, apparently collected in violation of DOD regulations and the Foreign Intelligence Surveillance Act (FISA).

According to news reports, DOD has developed one or more databases of information on domestic persons, including "the monitoring of peaceful anti-war and counter-military recruitment groups."¹ According to this report, the DOD's information collection consists of "domestic intelligence that goes beyond legitimate concerns about terrorism or protecting U.S. military installations."² Furthermore, it is reported that such information is retained in DOD's databases even after it has been deemed irrelevant to combating terrorism or protecting military facilities.³ The report indicates that DOD's purpose in collecting and retaining this information is in part to further a data mining project conducted by DOD's Counterintelligence Field Activity (CIFA) agency, based at least in part on Threat and Local Observation Notice (TALON) reports.⁴

I am concerned that the information collected and retained by DOD may have been collected in violation of its own regulations and in violation of FISA. The reports do not indicate that the information DOD has collected on U.S. persons has been obtained pursuant to a court order or that it is publicly available information. If true, these activities could violate FISA's general stipulation that searches of U.S. persons, whether electronic or physical, be performed pursuant to a court-ordered warrant upon a determination of probable cause.⁵ This could also violate

¹ "Is the Pentagon Spying on Americans," MSNBC News, Lisa Myers *et al.*, Dec. 14, 2005 (available at <http://msnbc.msn.com/id/10454316/>).

² *Id.*

³ *Id.*

⁴ *Id.*

⁵ See 50 U.S.C. §§ 1802, 1804; 1822, 1824.

FISA's stipulation that DOD's surveillance and search activities collect foreign intelligence information, rather than target domestic speech activities protected by the First Amendment. FISA's provisions authorize surveillance and searches for the gathering specifically of foreign intelligence information, not any information that DOD decides to collect.⁶ FISA's provisions also make clear that probable cause to conduct surveillance or searches of a U.S. person cannot rest solely on that person's activities protected by the First Amendment.⁷ If the reports are accurate, it appears that DOD may have specifically targeted U.S. persons based upon their activities protected by the First Amendment.

DOD's regulations implementing FISA's statutory requirements also underscore the general need for DOD to obtain lawful court orders prior to conducting domestic intelligence activities. DOD's regulations generally require the use of "overt" means of intelligence gathering on U.S. persons, where the subject is advised or otherwise aware that he or she is providing intelligence information to DOD. The use of covert intelligence gathering on U.S. persons is circumscribed to a very narrow set of circumstances, none of which appear to apply here if news reports are correct.⁸ Indeed, DOD's intelligence gathering here appears to have targeted the domestic activities of U.S. persons, for which covert means are impermissible.⁹ DOD's regulations also permit intelligence gathering on U.S. persons only for specific types of information, none of which appear to apply here. In pertinent part, DOD's rules generally permit the collection of non-consensual, non-public information for foreign intelligence or counterintelligence purposes, and for the protection of military facilities.¹⁰ DOD's rules permit non-consensual physical surveillance of U.S. persons within the United States only if the subject has a specified employment or contractual relationship with the military or intelligence services.¹¹ Intelligence gathering on peaceful domestic anti-war and counter-military recruitment groups does not appear to fall within any of these categories. Moreover, DOD's data mining of such intelligence information on U.S. persons collected in violation of its rules generally would contravene DOD's rules against retention of such information.¹²

I ask that you immediately begin an investigation of these alleged violations of the law and report your findings to me by January 31, 2006. In particular, your report should contain the following information:

(1) What types of information has DOD collected on U.S. persons? What types of information has DOD collected on U.S. persons belonging to domestic anti-war or counter-military recruitment groups?

(2) What overt methods has DOD employed to collect this information? What non-overt methods has DOD employed to collect this information?

⁶ *See id.*

⁷ *See, e.g.*, 50 U.S.C. §§ 1804(a)(3)(A); 1824(a)(3)(A).

⁸ *See* DOD 5240 1-R, "Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons," at Procedure C2.5.

⁹ *See id.* at Procedure C2.5.1.

¹⁰ *See id.* at Procedure C2.3.

¹¹ *See id.* at Procedure C9.3.1.

¹² *See id.* at Procedure C3.3.

(3) What types of information on U.S. persons does DOD store as part of its CIFA or TALON programs?

(4) On how many distinct U.S. persons has DOD collected information? On how many distinct U.S. persons does DOD currently retain information?

(5) On how many distinct U.S. persons consisting of or belonging to domestic anti-war or counter-military recruitment groups has DOD collected information? On how many such persons does DOD currently retain information?

(6) For information on U.S. persons retained by DOD, provide a percentage breakdown of the amount of data points collected pursuant to each prong of Procedure 2.3. For information retained by DOD on U.S. persons who belong to domestic anti-war or counter-military recruitment groups, provide a percentage breakdown of the amount of data points collected pursuant to each prong of Procedure 2.3.

(7) Where non-public information on U.S. persons has been collected without their consent, has DOD in every instance obtained a warrant from a court of lawful jurisdiction? If not, on what legal authority has DOD obtained this information in each instance, and how is this information collection consistent in each instance with DOD 5240 1-R?

Please contact Praveen Goyal of my staff at (202) 225-3072 to coordinate providing your report to me by January 31, 2006, including answers to the specific questions posed above. Thank you for your urgent attention to this serious matter.

Sincerely,



Zoe Lofgren
Member of Congress

Appendix C. Congressional Request from Congresswoman Anna G. Eshoo



*Congress of the United States
House of Representatives
Washington, D.C. 20515*

*Anna G. Eshoo
Fourth District
California*

January 12, 2006

Mr. Thomas E. Gimble, Acting Inspector General
Department of Defense
400 Army-Navy Drive
Arlington, Virginia 22202

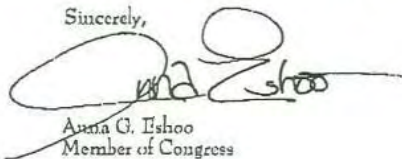
VIA FACSIMILE

Dear Inspector General Gimble,

I'm writing to request your assistance in determining the veracity of media reports concerning Department of Defense (DoD) activities on a university campus in California. The Chancellor of the University of California, Santa Cruz (UCSC) recently contacted me to express her great concern about media reports that the DoD was conducting an investigation of a peaceful campus protest at UCSC. I, too, am deeply concerned about such reports, given our country's past mistakes of conducting surveillance of patriotic Americans during times of war.

I'm aware that Under Secretary of Defense for Intelligence Stephen A. Cambone has notified the House Permanent Select Committee on Intelligence that he has directed a review of all DoD policies and procedures regarding the Department's collection, retention, and use of domestic information. I've written to Dr. Cambone, asking him to keep me personally informed of the Department's findings and actions. I also am hereby requesting you to look specifically into the DoD activities at UCSC and report your findings to me as soon as possible.

Sincerely,



Anna G. Eshoo
Member of Congress

Enclosures

cc. Denise D. Denton, Ph.D., Chancellor
University of California, Santa Cruz



Message to UC Santa Cruz Staff and Faculty
Wednesday, December 28, 2005

To: UCSC Campus Community
From: Denice D. Denton, Chancellor
David S. Kiger, EVC and Campus Provost

We are greatly concerned about the Pentagon's investigation of a UCSC campus protest of military recruiters last spring. MSNBC reports that this protest was classified as a "credible threat" by the Department of Defense.
(<http://www.msnbc.msn.com/id/10454316/>)

We have contacted our federal elected officials to express our concern. We are asking them to investigate the reported secret monitoring on college campuses. Investigating our campus protest - one among many around the country -- is a questionable use of military resources. It is especially disquieting that political dissent would be considered threatening.

We are at an important juncture in our history, and we urge the citizenry and the leadership to recall the mistakes of the past in times of war, especially with respect to the expansion of executive power. As a nation, we must be vigilant and careful in balancing the competing needs of national security and the fundamental rights and values of individuals in a free and democratic society.

An environment of surveillance and intimidation threatens the core values of universities and of our nation. As educators, we must stand vigorously against such intrusions. It is our job as a university to create a learning environment in which students, staff, and faculty can explore the widest range of ideas available to them, express a full range of opinions, and exercise a complete spectrum of political rights, up to and including the rights of peaceful protest and political expression.

We would be abdicating our responsibility as educators if we fail to nurture a learning environment in which all points of view can be expressed and listened to with respect. While we do not tolerate violence, peaceful protests are one important way to help build a better society. Diversity of opinion, as with other forms of diversity and difference, is a hallmark of excellence that distinguishes UC Santa Cruz and other great institutions of higher education.



*Congress of the United States
House of Representatives
Washington, D.C. 20515*

*Anna L. Eshoo
Fourth District
California*

January 12, 2006

The Honorable Stephen A. Cambone
Under Secretary of Defense for Intelligence
Department of Defense
1000 Defense Pentagon
Washington, D.C. 20301-1000

VIA FACSIMILE

Dear Under Secretary Cambone,

I'm deeply concerned about recent media reports that the Department of Defense (DoD) is conducting investigations of campus protests across the country, including those at the University of California, Santa Cruz (UCSC). If these disturbing reports are true, these actions are inconsistent with important First Amendment rights and cherished civil liberties guaranteed to all Americans.

I have reviewed your letter to the House Permanent Select Committee on Intelligence informing us that you have directed a review of all DoD policies and procedures regarding the collection, retention, and use of domestic information. Many questions, however, remain. I therefore request that, in addition to keeping the Committee fully informed of the results of your review, you provide answers to the following questions:

- Has any DoD official authorized the collection of information related to student protests? If so,
 - Who authorized these activities?
 - What was the legal basis for this authorization?
 - What types of activities were authorized?
 - What are the guidelines governing the collection, retention and dissemination of the information collected?
- Has DoD engaged in any operational activities against students as a result of their alleged participation in protests on or off campus? If so, please describe these activities.



Appendix D. Response to Congresswoman Lofgren

In a letter to the DoD IG dated December 30, 2005, Congresswoman Lofgren asked seven questions about U.S. person information contained in the TALON reports that specifically related to domestic anti-war or counter-military protests and demonstrations and the legal basis for the TALON reports.

Congresswoman Lofgren's request mentioned a possible violation of the Foreign Intelligence Surveillance Act (FISA) and also detailed information on retaining information regarding U.S. persons. To adequately answer the request, we included the following background information on FISA and the methodology we used to categorize U.S. person information.

FISA. Public Law 95-511, "Foreign Intelligence Surveillance Act of 1978," October 25, 1978 (as amended), provides a statutory structure to be followed where electronic surveillance, physical searches, or pen registers or trap devices for foreign intelligence gathering purposes are contemplated. FISA creates enhanced procedural protections, where a U.S. person is involved, to protect personal liberties safeguarded by the First and Fourth Amendments while providing a means to protect national security interests. The Act provides for surveillance of American citizens and others for whom the court determines that there is probable cause that they are "agents of a foreign power" as defined in the statute. The Act sets up a Foreign Intelligence Surveillance Court to authorize such surveillance.

None of the TALON reports reviewed were created as the result of intelligence surveillance. The TALON reports were developed from information provided to security, law enforcement personnel at military facilities, and/or intelligence personnel. The information was primarily from concerned individuals such as citizens; military personnel, both performing their official duties and as citizens; and law enforcement personnel. Therefore, FISA does not apply to the TALON reports.

U.S. Person. Our definition of a U.S. person was primarily designed to provide an accurate response to the intent of the congressional questions. We did not include U.S. person information in the TALON reports that identify ancillary personnel. For example, we did not include the people who provided or handled the information, most of whom were Government employees, or consider data related to victims, sources of information, witnesses and report creators as U.S. person information.

For example, if a TALON report stated:

John Doe witnessed a man throw an object at the DoD IG building, then jump into a blue Chevy sedan and speed away down Army Navy Drive. The Chevy turned left just past the Embassy Suites.¹¹

We would have determined there was no U.S. person information because John Doe was the witness who reported the incident so the information was obtained with consent, Chevy was the type of car not a company we are interested in, and Embassy Suites is just a point of reference not a business being identified.

Question 1. What types of information has DoD collected on U.S. persons? What types of information has DoD collected on U.S. persons belonging to domestic anti-war or counter-military recruitment groups?

Answer. Any information that pertains to a U.S. person is U.S. person information; however, if a U.S. person is not identified, the same information is not U.S. person information. Therefore, all potential U.S. person information must be reviewed and a U.S. person identified before the final decision can be made as to what is U.S. person information in each report.

This audit reviewed only the records generated as part of the TALON program. Of the 1,131 TALON reports deleted by CIFA from December 2, 2005, through January 18, 2006, the audit identified 263 TALON reports related to protests and demonstrations. U.S. person information was present in 92 of those reports. The information included in the TALON reports that we reviewed pertain to subjects; sources; witnesses; victims; interviewees; illegal aliens; famous people referenced for quotes, positions and scheduled appearances; law enforcement officials involved; and the agent creating the TALON. As discussed in Table 2 of the report, not all types of information included in the reports identify U.S. persons.

The TALON reports were manually reviewed by CIFA and DoD IG personnel. Many CIFA personnel reviewed the 1,131 TALON reports from September 2005 through January 2006, and identified 186 TALON reports that referenced “protest” and “demonstration.” Our review, which was performed by one auditor to ensure consistency, also included TALON reports that discussed vandalism, destruction, theft, and/or violence against a recruitment center or a recruiter as protests and demonstrations. We identified 263 protest and demonstration TALON reports rather than the 186 identified by CIFA, because we read all TALON reports and did not just search for the terms “protest” and “demonstration.” The inconsistency created by the multiple personnel involved in the CIFA review and the difference in the definition of protest and demonstration TALON reports also affected the difference in the numbers.

All TALON Reports. We identified six types of potential U.S. person information and the categories in the TALON reports reviewed. Table 3 shows the six types.

¹¹ This example was created to demonstrate the difference between the determinations made by CIFA and the DoD IG. This is not a real TALON report.

Table 3. Types and Categories of Potential U.S. Person Information

Types	Categories
Names	Individual: social security number, date of birth, place of birth, and/or descriptions (sex, hair color, height, weight, nationality, ethnical appearance), and/or position or title or rank* Organization or group Business or company
Addresses	Street, city, and/or state
Phone numbers	Home, work (business or company), and/or cell
Vehicles	Descriptions: color, model, and/or distinguishing factors License plates: state and/or number Owner (see names)
E-mail addresses	
Websites	

* Any of these categories may be recorded without the name of the individual.

Protests and Demonstrations. The types of information contained in the TALON reports on protests and demonstrations included the names of individuals and organizations, phone numbers, addresses, e-mail addresses and websites associated with the protestors. Phone numbers and addresses were only recorded when it was contained in an e-mail or website as a contact reference. Recorded e-mail addresses were obtained from the e-mail sender or provided in an e-mail or website as a contact reference. Websites were recorded when they were provided in an e-mail as an information source.

Question 2. What overt methods has DoD employed to collect this information? What non-overt methods has DoD employed to collect this information?

Answer. DoD did not employ either overt or covert intelligence methods to obtain the information contained in the TALON reports. Our review of the source information contained on each TALON report indicated they were developed from information provided to the security and law enforcement personnel at military facilities, and/or intelligence personnel. The information was from concerned individuals such as civilians; military personnel, both performing their official duties and as citizens; and law enforcement personnel. Concern arises when individuals hear, see, or are informed about suspicious incidents being

planned, that happen at a military facility, or that involve military personnel. Concern also arises when citizens see suspicious activity and don't know what to do about it. Most citizens in the vicinity of military facilities knew a member of the military or another individual working for or with the DoD. These individuals reported suspicious incidents to DoD contacts rather than through formal law enforcement channels.

TALON reports were established to create an avenue for reporting all types of suspicious incidents to DoD personnel, facilities, and resources. Additional information was added to reports if the results were posted or if the incident required followup or investigation for law enforcement purposes.

U.S. person information contained in the TALON reports was not reported for intelligence purposes. The information was collected for law enforcement and force protection purposes. Even the TALON reports generated by the Army 902d Military Intelligence Group from information received from a special agent of the Federal Protective Service, Department of Homeland Security was not intelligence information because it was provided for law enforcement and force protection purposes.

Question 3. What types of information on U.S. persons does DoD store as part of its CIFA or TALON programs?

Answer. Table 3 summarizes the type of U.S. person information in the TALON reports. The Cornerstone database included about 13,000 TALON reports, as of December 2005. As discussed in the report, the database was extensively reviewed to delete TALON reports that no longer had an analytical value as well as those initially deleted from December 2, 2005, through January 18, 2006.

The number of TALON reports being created decreased significantly after the Deputy Secretary Defense issued the March 30, 2006, memorandum, "Threats to the Department of Defense," which directed that the TALON Reporting System should report only information on possible international terrorist activity. Currently, all TALON reports are being retained in accordance with DoD Regulation 5240.1-R, "Activities of DoD Intelligence Components That Affect United States Persons," December 1982.

In January 2007, Cornerstone was queried for the number of TALON reports received each month. TALON reports deleted from Cornerstone were not included in the counts, which would understate the number of TALON reports received. On average, 49 TALON reports were submitted each month in the 13 months prior to the March 30, 2006, Deputy Secretary of Defense memorandum. However, since then, the average dropped to seven TALON reports each month.

The USNORTHCOM JPEN deleted all TALON reports on November 30, 2005, and the system was turned off in June 2006. This system did not have the capability to archive records; as a result, all of the information was lost.

Question 4. On how many distinct U.S. persons has DoD collected information? On how many such persons does DoD currently retain information?

Answer. We reviewed all of the 1,131 TALON reports that were deleted from December 2, 2005, through January 18, 2006, and found that DoD reported and maintained information on 571 U.S. persons in 334 TALON reports (Table 1). Table 4 (Table 2 in the finding discussion, repeated here) shows the number of U.S. persons identified by category for the 334 reports.

Table 4. U.S. Persons Identified in the 334 TALON Reports

	Protests and Demonstrations (92 Reports)	Others (242 Reports)	Total
Individuals	38	342	380
Organizations	104	6	110
Company or business		81	81
Total	142	429	571

The TALON reports currently in the Cornerstone database were reviewed by CIFA analysts who determined there is a reasonable belief that a link exists with “international terrorist activity.” The TALON reports contain actions such as tests of security and surveillance.

Question 5. On how many distinct U.S. persons consisting of or belonging to domestic anti-war or counter-military recruitment groups has DoD collected information? On how many distinct U.S. persons consisting of or belonging to domestic anti-war or counter-military recruitment groups does DoD currently retain information?

Answer. Of the 263 TALON reports on protests and demonstrations in the United States, 92 (Table 1 in the report) identified 142 U.S. persons (38 individuals and 104 groups or organizations) (Table 2 repeated above). The other 171 reports on protests and demonstrations did not identify any U.S. person information or distinct organizations or individuals.

Question 6. For information on U.S. persons retained by DoD, provide a percentage breakdown of the amount of data points collected pursuant to each prong of Procedure 2.3. [DoD Regulation 5240.1-R] For information on U.S. persons who belong to domestic anti-war or counter-military recruitment groups retained by DoD, provide a percentage breakdown of the amount of data points collected pursuant to each prong of Procedure 2.3.

Answer. Prior to March 30, 2006, the U.S. person information in TALON reports was not reported or maintained for intelligence purposes, as directed by Executive Order 12333, "United States Intelligence Activities," December 4, 1981, with implementation by DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," December 1982. Rather, the information was reported and maintained for law enforcement as authorized by DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense," January 7, 1980. Therefore, we cannot provide percentage breakdown of the information collected by Procedure 2.3 of DoD Regulation 5240.1-R

Question 7. Where non-public information on U.S. persons has been collected without their consent, has DoD in every instance obtained a warrant from a court of lawful jurisdiction? If not, on what legal authority has DoD obtained this information in each instance, and how is this information collection consistent in each instance with DoD 5240 1-R?

Answer. Non-public information was collected when criminal checks were run on subjects of potentially criminal actions. The TALON reports for protests and demonstrations did not contain non-public information; we determined that any name, phone number, address, or e-mail address provided as a point of contact in an e-mail, website, flier, brochure, or newspaper article is public information. The TALON reports were developed based on the Deputy Secretary of Defense memorandum, "Collection, Reporting, and Analysis of Terrorist Threats to DoD Within the United States," May 2, 2003. The memorandum wanted input of non-validated, domestic, suspicious activity from intelligence, counterintelligence, law enforcement, and force protection sources. No other DoD TALON policies or guidance were issued prior to March 2006. The Services developed implementation policy that treated TALON reports as a law enforcement tool. DoD TALON reports, including those on protests and demonstrations, were generated for law enforcement and force protection purposes, not for intelligence purposes. Collection of such data for law enforcement or force protection is permitted under DoD Directive 5200.27.

Appendix E. Response to Congresswoman Eshoo

In a letter to the DoD IG dated January 12, 2006, Congresswoman Eshoo requested that the DoD IG look into DoD activities at the University of California, Santa Cruz (UCSC) after the Chancellor of UCSC contacted her with concerns about the media reports that DoD was conducting an investigation of a peaceful campus protest at UCSC.

Question. I am hereby requesting you to look specifically into the DoD activities at the University of California, Santa Cruz (UCSC) and report your findings to me as soon as possible.

Answer. The only UCSC protest reported in TALON reports was the protest against military recruiters that occurred on April 5, 2005. We examined all of the TALON reports related to this protest. Two reports specifically discussed the UCSC protest, and two other reports referenced the UCSC protest as an example of why military recruiters needed to be careful.

One TALON report announced the planned protest at UCSC and warned that recent protests along the West Coast have drawn an estimated 200 to 400 protesters, with one incident in January 2005 resulting in police escorting the military recruiters off the campus. A second TALON report followed up on the protest at UCSC and stated that the protesters overpowered security at the event and that UCSC staff escorted the recruiters out of the area for their safety.

Two TALON reports are notification of weekly planned protests at the Atlanta, Georgia recruiting offices. These TALON reports use the UCSC protest to warn recruiters about a group involved because nearly 300 UCSC students and community allies shut down the annual career fair and demanded that recruiters leave. In addition, two of the recruiters' cars were vandalized while parked on the UCSC campus.

A comparison of the TALON reports with newspaper reports of the UCSC protest shows nearly identical details (300 protesters, a career-center staffer slightly injured, and some tires of the recruiters' cars were slashed), which validate the accuracy of the TALON report details. The newspaper reports also verify why the TALON reports are required for law enforcement and force protection purposes, and as law enforcement records, they are created and maintained legally.

Appendix F. Deputy Secretary of Defense May 2, 2003, Memorandum



~~FOR OFFICIAL USE ONLY~~

DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

HRS (UPR)



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~~

322

~~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~~

323

Appendix G. Deputy Secretary of Defense March 30, 2006, Memorandum



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.



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"

Appendix H. Deputy Secretary of Defense October 12, 2006, Memorandum



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

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 fluid and cursive, with the first name "Andrew" and last name "England" clearly distinguishable.

Attachment:
Updated TALON Reporting System Procedures

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.

-
- 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.

Appendix I. Deputy IG for Intelligence

June 20, 2006, Memorandum



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

JUN 20 2006

MEMORANDUM FOR SECRETARY OF THE AIR FORCE
DIRECTOR, JOINT STAFF

SUBJECT: The Joint Protection Enterprise Network Operation and Funding

We are providing this memorandum to alert you about the shutdown of the Joint Protection Enterprise Network (JPEN) database that may impact dissemination of potential threat information to DoD personnel, facilities, and resources. The U.S. Northern Command (USNORTHCOM) assumed oversight of JPEN from the Joint Staff in December 2003 without a resource sponsor or executive agent. Immediate action is needed to provide funding of \$690,975 to reactivate the system through the end of the fiscal year, until a funding source is identified.

We identified this issue as part of our ongoing audit of the Threat and Local Observation Notice (TALON) Report Program (Project No. 2006-DINT02-0128), being performed in response to Congressional requests that the Inspector General investigate "allegations that the Department of Defense (DoD) has developed and maintains a database of information on United States persons, apparently collected in violation of DoD regulations and the Foreign Intelligence Surveillance Act." As background, the May 2, 2003, Deputy Secretary of Defense memorandum stated that a TALON report was 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. Specifically, a TALON report was to consist of raw information reported by concerned citizens and military members regarding suspicious incidents. TALON reports were to be generated by all DoD intelligence, counterintelligence, law enforcement and security organizations with the mission to collect force protection and threat information. The plan for TALON reporting was for organizations to submit TALON reports to JPEN (available via the NIPRNET) and for the Counterintelligence Field Activity "Cornerstone" database (available via the SIPRNET) to import the reports directly from JPEN.

The "Unified Command Plan," June 30, 2002, creates USNORTHCOM and assigns it the mission of defending the United States and supporting the full range of military assistance to civil authorities. JPEN is the only DoD system that provides situational awareness of suspicious activity (foreign, domestic, and criminal) for all DoD elements (Services and Agencies) down to the installation level in the USNORTHCOM area of responsibility. A JPEN Suspicious Activity Report documents an act or acts that represent activity out of the ordinary, an anomaly to normal behavior, or activity that may be related to terrorism, criminal activity, or to other illicit activity that meets the authorized criteria set forth in DoD Directive 5200.27, "Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense," January 7, 1980, as a threat to DoD personnel, functions and property.

JPEN bridges the gap between suspicious activity occurring at one installation and knowledge of the potential threat at other installations and headquarters, with near-real-time reporting for quick analysis and action. Its development has been completed and the system has

~~FOR OFFICIAL USE ONLY~~

been fielded to over 1,900 users at over 400 installations and organizations across the USNORTHCOM area of responsibility.

USNORTHCOM assumed oversight of JPEN from the Joint Staff in December 2003 without a resource sponsor or executive agent. Since February 2006, USNORTHCOM has been responsible for funding JPEN out of existing command funds. There is no long-term funding strategy to sustain the JPEN program. Higher USNORTHCOM priorities make it impossible to sustain JPEN with USNORTHCOM resources. As a result, on June 13, 2006, the Commander, USNORTHCOM, signed a course of action to terminate the JPEN program as soon as possible.

Lack of JPEN capabilities will return TALON and suspicious activity reporting to status-quo stove-piped processes that result in delays and the inability of Combatant Command, Service, and Defense Agency commanders to collect, report, and share potential threats to DoD bases and facilities.

DoD Directive 5100.3, "Support of Headquarters of Combatant and Subordinate Joint Commands," November 15, 1999 (certified current as of March 24, 2004), requires the Secretary of the Air Force to provide or arrange for the administrative and logistic support of USNORTHCOM.

In order to maintain a capability to disseminate potential threat information to DoD personnel, facilities, and resources, JPEN must be operational. We also need access to JPEN to complete the Congressionally requested review. Therefore, we are recommending that the Secretary of the Air Force work with the Joint Staff to identify a funding source to provide \$690,975 to continue operation of the JPEN through the end of FY 2006.

We request immediate action and your comments to resolve the JPEN funding issue by July 7, 2006. This memo and your comments will be included in our report.



Shelton R. Young
Deputy Inspector General
for Intelligence

cc: COMMANDER, USNORTHCOM

~~FOR OFFICIAL USE ONLY~~

Appendix J. Director, Joint Staff July 24, 2006, Memorandum



THE JOINT STAFF
WASHINGTON, DC

Reply ZIP Code:
20318-0300

DJSM-0700-06
24 Jul 2006

MEMORANDUM FOR THE INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

Subject: Joint Protection Enterprise Network (JPEN) Operation and Funding

1. Thank you for your office's concern over subject operation and funding.¹ We agree this system is valuable in the collection, reporting, and sharing of potential threats to DOD infrastructure.
2. However, JPEN has experienced funding difficulties since its inception. In the past, these were overcome through sacrifices and tough decisions made by the US Air Force, Joint Staff, and USNORTHCOM. Unfortunately, today's budget pressures no longer allow the flexibility to continue funding JPEN shortfalls.
3. In the absence of a viable long-term funding strategy, I support CDRUSNORTHCOM's decision to shut down JPEN. If the command chooses to readdress this decision at a later date, the Joint Staff will reevaluate the requirement through the Joint Capabilities Integration and Development System process.

A handwritten signature in black ink, appearing to read "Walter L. Sharp".

WALTER L. SHARP
Lieutenant General, USA
Director, Joint Staff

Reference:

- 1 DIG for Intelligence memorandum, 20 June 2006, "The Joint Protection Enterprise Network Operation and Funding"

Copy to:
Air Force Operations Deputy
DCDRUSNORTHCOM

Appendix K. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Policy

Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs

Deputy Assistant Secretary of Defense for Homeland Defense

Under Secretary of Defense for Intelligence

Deputy Under Secretary of Defense (Counterintelligence and Security)

General Counsel of the Department of Defense

Assistant to the Secretary of Defense (Intelligence Oversight)

Joint Staff

Director, Joint Staff

Department of the Army

Auditor General, Department of the Army

Commanding General, U.S. Army Intelligence and Security Command

Provost Marshall General

Commanding General, U.S. Army Criminal Investigation Command

Department of the Navy

Naval Inspector General

Auditor General, Department of the Navy

Director, Naval Criminal Investigative Service

Department of the Air Force

Auditor General, Department of the Air Force

Commander, Air Force Office of Special Investigations

Combatant Command

Commander, U.S. Northern Command

Inspector General, U.S. Northern Command

Inspector General, U.S. Joint Forces Command

Other Defense Organizations

Director, Counterintelligence Field Activity
General Counsel, Counterintelligence Field Activity

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
Senate Select Committee on Intelligence
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Oversight and Government Reform
House Subcommittee on Government Management, Organization, and Procurement,
Committee on Government Reform
House Subcommittee on National Security and Foreign Affairs, Committee on Oversight
and Government Reform
House Committee on Homeland Security
House Permanent Select Committee on Intelligence

Counterintelligence Field Activity Comments



COUNTERINTELLIGENCE FIELD ACTIVITY
251 18th STREET
CRYSTAL SQUARE 5, SUITE 1200
Arlington, VA 22202-3537




JUN 04 2007

MEMORANDUM FOR DEPUTY ASSISTANT INSPECTOR GENERAL FOR
INTELLIGENCE AUDITS

SUBJECT: Threat and Local Observation Notice (TALON) Report Program
(Project No. 2006-DINT01-0128.000)

Following review of subject report, CIFA provided substantive comments that have been incorporated into the draft proposed report. Although CIFA anticipates the TALON program will be terminated in the future, this report will assist the Assistant Secretary of Defense (Homeland Defense) in crafting an efficient and effective suspicious activity reporting system if the Department decides that is the course of action for the way ahead.


James T. Faust
Director

cc:
DUSD (CI&S)
DOD GC (Intelligence)

Team Members

The Department of Defense Office of the Deputy Inspector General for Intelligence prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Shelton R. Young
Sean Mitchell
Lois A. Therrien
Averel E. Gregg
Dana Johnson
Tomica Q. May



Inspector General Department of Defense