

Inspector General

United States
Department of Defense



Report No. 07-INTEL-14
September 28, 2007

DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

Review of Access to U.S. Persons Data by the Space and Naval Warfare Systems Command (U)

Special Warning

This document contains information exempt from mandatory disclosure under the Freedom of Information Act. (b)(1)

Reproduction or removal of pages is prohibited. Safeguards must be taken to prevent publication or improper disclosure of the information in this report.

(b)(1)

(U)

Additional Information and Copies

The Office of the Deputy Inspector General for Intelligence of the Department of Defense prepared this report. If you have questions on the report, or to request additional copies, contact (b)(6) (b)(6),(b)(1) (b)(1)

Suggestions for Audits

To suggest ideas for or to request future audits or evaluations of Defense Intelligence issues, 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
Inspector General of the Department of Defense
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 (U)

- ATSD (IO) Assistant to the Secretary of Defense for Intelligence Oversight
- DRT Digital Receiver Technology
- HITS Hostile Forces Integrated Targeting System
- ICWPA Intelligence Community Whistleblower Protection Act
- MOA Memorandum of Agreement
- NGA National Geospatial-Intelligence Agency
- NRO National Reconnaissance Office
- NSA National Security Agency
- (b)(1)
- ONI Office of Naval Intelligence
- (b)(1)
- SPAWAR Space and Naval Warfare Systems Command
- SSC-SD Space and Naval Warfare Systems Center San Diego



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

September 28, 2007

MEMORANDUM FOR THE ASSISTANT TO THE SECRETARY OF DEFENSE FOR
INTELLIGENCE OVERSIGHT

SUBJECT: Report on Review of Access to U.S. Persons Data by the Space and Naval
Warfare Systems Command (Report No. 07-INTEL-14) (U)

(U) We are providing this report for information and use. We performed the review in response to an Intelligence Community Whistleblower Protection Act allegation. We considered management comments on a draft of this report in preparing the final report. The Acting Assistant to the Secretary of Defense for Intelligence Oversight comments conformed to the requirements of DoD Directive 7650.3; therefore, additional comments are not required.

(U) We appreciate the courtesies extended to the staff. Questions should be directed to (b)(6) (b)(1), (b)(6) (b)(1). See Appendix D for the report distribution. The team members are listed inside the back cover.

Shelton R. Young
Deputy Inspector General
for Intelligence

Special Warning

This document contains information exempt from mandatory disclosure under the Freedom of Information Act. (b)(1)

(b)(1)

(b)(1)

Reproduction or removal of pages is prohibited. Safeguards must be taken to prevent publication or improper disclosure of the information in this report.

TOP SECRET (b)(1)

(U) THIS PAGE INTENTIONALLY LEFT BLANK (U)

Department of Defense Office of Inspector General

Report No. 07-INTEL-14
(Project No. D2007-DINTEL-0106)

September 28, 2007

Review of Access to U.S. Persons Data by the Space and Naval Warfare Systems Command (U)

Executive Summary (U)

(U) Who Should Read This Report and Why? DoD personnel, the Intelligence Community, and all personnel at research and development facilities performing work for DoD intelligence components should read this report. The report discusses the policy and procedures for accessing and handling information about U.S. persons collected by research and development facilities. A "U.S. person" is a U.S. citizen; an alien known by the DoD intelligence component concerned to be a permanent resident alien; an unincorporated association substantially composed of U.S. citizens or permanent resident aliens; a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

(TS) (b)(1) Background. On December 18, 2006, (b)(1) submitted an Intelligence Community Whistleblower Protection Act complaint that contained allegations about a lack of intelligence oversight procedures at research and development facilities performing work for DoD intelligence components. The employee specifically raised concerns about the perceived mishandling of U.S. persons information by the Space and Naval Warfare Systems Center San Diego, a research and development facility (b)(1). The employee also raised concerns that (b)(1) was not responsive to his request to investigate and correct the deficiencies associated with the Space and Naval Warfare Systems Center San Diego and other DoD research and development facilities. The employee also alleged that he was reprimed against for his actions.

(TS) (b)(1) Results. We did not substantiate the allegations that the Space and Naval Warfare Systems Center San Diego was mishandling intelligence and possibly compromising U.S. persons information, specifically through its use of (b)(1), (b)(1) and SPAWAR (b)(1) systems.

(TS) (b)(1) We partially substantiated the allegation that (b)(1) was not responsive to initiating action to investigate and correct the deficiencies associated with the Space and Naval Warfare Systems Center San Diego and other DoD research and development facilities. The corrective actions taken by (b)(1) were confined to validating the need for the Space and Naval Warfare Systems Center San Diego to (b)(1) and establishing an Intelligence Oversight program (b)(1). However, the actions taken by (b)(1) to identify and correct problems at other DoD research and development facilities have not been completed and we could not assess whether they will be effective.

(U//FOUO) We did not substantiate that (b)(1) was reprimed against for actions associated with the Space and Naval Warfare Systems Center San Diego.

Specific information regarding the actions are contained in a separate report issued by the DoD IG Director of Civilian Reprisals on September 26, 2007 (Appendix E.)

(U) The DoD has not established procedures for control or oversight of U.S. persons information that may be obtained by DoD research and development facilities. The DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982, (DoD Regulation 5240.1-R) does not include DoD research and development facilities. We recommended that the regulation be modified to require DoD research and development facilities to safeguard and report for intelligence oversight purposes if U.S. persons data is collected.

(U//~~FOUO~~) Management Comments and DoD IG Response. The Acting Assistant to the Secretary of Defense for Intelligence Oversight concurred with the recommendations; therefore, no further comments are required. See the Finding section of the report for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.

Table of Contents (U)

(U)

Executive Summary	i
Background	1
Objectives	2
Finding	
Access to U.S. Persons Information at DoD Research and Development Facilities	3
Appendixes	
A. Scope and Methodology	12
Prior Coverage	13
B. Intelligence Community Whistleblower Protection Act	
C. DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982 Intelligence Community Whistleblower Protection Act	14
D. Report Distribution	16
E. Report of Investigation of Alleged Reprisal (b)(1)	19
Management Comments	
Assistant to the Secretary of Defense for Intelligence Oversight	35

~~TOP SECRET~~

(b)(1)

THIS PAGE INTENTIONALLY LEFT BLANK (U)

~~TOP SECRET~~

(b)(1)

Background (U)

(TS//~~(S)~~) **Allegations.** On December 18, 2006, (b)(1) submitted an Intelligence Community Whistleblower Protection Act (ICWPA) complaint that contained allegations about a lack of training and intelligence oversight procedures at DoD research and development facilities performing work for intelligence components. The employee specifically raised concerns about the perceived mishandling of U.S. persons' information by the Space and Naval Warfare Systems Center San Diego (SSC-SD), a research and development facility (b)(1). Specifically, the complainant alleged that SSC-SD:

(b)(1)

- Was photographing U.S. persons.

The employee also indicated that the problems might not be confined to SSC-SD and that similar deficiencies could be occurring at other DoD research and development facilities.

(U//~~(S)~~) Further, the employee alleged (b)(1) was not responsive to initiating action to investigate and correct the deficiencies associated with SSC-SD and other DoD research and development facilities. The employee also alleged he was reprimanded against for reporting the need to correct these deficiencies (b)(1). The DoD IG Director of Civilian Reprisal review did not substantiate the allegation. The report of investigation is included as Appendix E.

(TS//~~(S)~~) **SSC-SD.** The SSC-SD is one of five field activities of Space and Naval Warfare Systems Command (SPAWAR) that provides tactical and non-tactical information management technology required by the Navy to complete its operational missions. The SSC-SD provides information resources to support the joint war-fighter in mission execution and force protection. The SSC-SD designs,

¹(U) For a detailed discussion of the ICWPA process, see Appendix B.

²(U) A "U.S. person" is a U.S. citizen; an alien known by the DoD intelligence component concerned to be a permanent resident alien; an unincorporated association substantially composed of U.S. citizens or permanent resident aliens; a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. See DoD Regulation 5240.1-R, Definitions.

builds, tests, fields, and supports command, control, communications, computers, intelligence, surveillance, and reconnaissance systems. In addition to work performed for the Navy, SSC-SD conducts research and development for the Defense Intelligence Components. During 2007^{(b)(1)}, 23 projects for the National Reconnaissance Office (NRO), and seven projects for the National Geospatial-Intelligence Agency (NGA). Headquarters SSC-SD is located on the Point Loma peninsula in San Diego, California.

Objectives (U)

(U//~~FOUO~~) The overall objective was to determine if U.S. persons information was controlled in accordance with applicable laws and regulations. Specifically, we reviewed if access to the U.S. persons information by the SSC-SD is required, controlled, and reported. We also determined if^{(b)(1)} took appropriate actions once informed of the allegations of potential mishandling of U.S. persons information. We were planning a separate review of the access to the U.S. persons information at other DoD research and development facilities. However, based on the results of our work performed on this review, we have determined that we can address the need for intelligence oversight programs at DoD research and development facilities in this report.

Access to U.S. Persons Information at DoD Research and Development Facilities (U)

(TS) (b)(1) We did not substantiate allegations that SSC-SD was mishandling intelligence and possibly compromising U.S. persons information, specifically through its use of (b)(1) SPAWAR (b)(1) systems. We partially substantiated the concern that (b)(1) did not initiate action to investigate and correct the deficiencies associated with SSC-SD and other DoD research and development facilities in a timely manner. The actions taken by (b)(1) were confined to validating the need for SSC-SD to (b)(1) and establishing an intelligence oversight program (b)(1). The actions taken to identify and correct problems at other DoD research and development facilities have not been completed and we could not assess whether they will be effective. DoD has not established sufficient procedures for control or oversight of U.S. persons information that may be obtained by research and development facilities. As a result, U.S. persons data, if collected by a DoD research and development facility, may not be safeguarded or reported in accordance with DoD Regulation 5240.1-R.

SSC-SD Access to U.S. Persons Information (U)

(TS) (b)(1) We did not substantiate allegations that the SSC-SD was mishandling intelligence and compromising U.S. persons information, specifically through its (b)(1) SPAWAR (b)(1) systems. We reviewed (b)(1) SPAWAR (b)(1) related projects at SSC-SD and did not find any instances in which U.S. persons information was being inappropriately handled. We found no specific instances in which (b)(1) SPAWAR (b)(1) was primarily used to (b)(1) in those cases in which SPAWAR (b)(1) was used, appropriate approvals were obtained in advance, and U.S. Government facilities, not U.S. persons, were targeted.

(b)(1) Access (U)

(TS) (b)(1) We did not validate that SSC-SD obtained (b)(1)

(b)(1) **Collection (U)**

~~(TS)~~ (b) We did not substantiate the concern that SSC-SD was (b)(1)

[Redacted]

~~(TS)~~ (b) We found that SSC-SD obtained approval to collect (b)(1)

[Redacted] (b)(1)

~~(TS)~~ (b) We believe there may have been a misperception concerning requests by SSC-SD for (b)(1)

[Redacted]

(b)(1)

~~(TS)~~ (b) We did not substantiate the allegation that SSC-SD was collecting U.S. persons information (b)(1)

[Redacted]

[Redacted]

4 ~~(TS)~~ (b) (b)(1)

5 ~~(TS)~~ (b) (b)(1)

[Redacted]

(b)(1)

(S) (b) (b)(1)

Imagery (U)

(TS) (b) (1) San Diego Harbor (b)(1) We found no evidence that SSC-SD was either SPAWAR (b)(1) or making SPAWAR (b) of U.S. persons. We believe the complainant misunderstood the SSC-SD research and development effort, (b)(1) being performed for the Office of Naval Intelligence (ONI). (b)(1)

(b)(1) SPAWAR (b)(1) (b)(1)

(TS) (b) (1) The SSC-SD tests systems prior to deploying them (b)(1). The test location is on Point Loma and overlooks San Diego harbor. During the tests, (b)(1)

(b)(1) SPAWAR (b)(1) The system's capability to produce SPAWAR (b)(1) and SPAWAR (b)(1) is used at SPAWAR (b)(1) at SSC-SD. The SSC-SD personnel indicated that SSC-SD made only one SPAWA (b)(1). The SPAW (b)(1) was made at the request of the Navy and was made of the USS Dolphin, a Navy submarine, after it had been repaired for fire damage. The SSC-SD does not retain copies of the SPAWA (b)(1) files on the system. We reviewed data stored on the system at the time of our review and did not find any inappropriate images.

(TS) (b) (1) Other Imaging. We did not substantiate that SSC-SD was collecting data on U.S. persons in Federal parks located at Point Loma, California without notice, warrant, or authority. We observed that SSC-SD has a camera and antenna mounted to a tower at their headquarters facility. The SSC-SD uses the camera and antenna for calibration purposes by pointing them at several different government radars.

The camera can be rotated 360 degrees. The video feed from the camera goes to a monitor in its laboratory. The images are not recorded and are not used to inappropriately monitor U.S. persons.

~~(TS)~~ (b) (1) **Satellite Imagery.** The SSC-SD properly obtained SPAWAR (b)(1) imagery of locations within the U.S. The imagery was needed in support of (b)(1) SPAWAR (b)(1) and in support of exercise SPAWAR (b)(1).⁶ The imagery was needed to demonstrate whether SPAWAR (b)(1) imagery of the location (b)(1)

(b)(1) NGA (b)(1)

Personnel at SSC-SD also submitted test plans for the exercises. However, there was no intelligence oversight reporting or monitoring of the imagery aspects of these tests and exercises.

(b)(1) **Actions (U)**

~~(TS)~~ (b) (1) We partially substantiated the concern that (b)(1) did not initiate action to investigate and correct the deficiencies associated with SSC-SD and other DoD research and development facilities. (b)(1) did not promptly assess the situation at SSC-SD. Further actions taken (b)(1) were confined to validating the need for SSC-SD to (b)(1) and establishing an intelligence oversight program (b)(1) has not completed actions recommended (b)(1) to identify and correct problems at other DoD research and development facilities. We could not assess whether (b)(1) actions will be effective.

Actions Related to SSC-SD (U)

~~(TS)~~ (b) (1) (b)(1)

⁶(b)(1)

(b)(1) [Redacted]

(b)(1) [Redacted]

(TS) (b) (b)(1) [Redacted]

(TS) (b) (b)(1) [Redacted]

(TS) (b) (b)(1) **Intelligence Oversight Reporting.** (b)(1) to initiate an intelligence oversight program (b)(1) at SSC-SD, a DoD research and development facility. (b)(1)

[Redacted]

provides oversight (b)(1), it does not establish a comprehensive intelligence oversight program over all SSC-SD activities (b)(1)

[Redacted]

one of these DoD intelligence components are required to be notified if there are reportable occurrences associated with their projects.

(TS) (b) (b)(1) **Counterintelligence Scope Polygraphs.** The SSC-SD initiated action to have all appropriate personnel consent to have counterintelligence scope polygraphs. The SSC-SD initiated action to have the counterintelligence scope polygraphs completed. As of August 2007, (b) SSC-SD personnel successfully completed polygraph examinations. An additional (b) SSC-SD personnel signed consent to polygraph examination forms but have not been examined. The SSC-SD was dependent on personnel from the Naval Criminal Investigative Service to perform the polygraphs.

⁷ (C) (b)(1) [Redacted]

(b)(1) [Redacted]

According to SSC-SD personnel, the Naval Criminal Investigative Service has significant backlogs due to increased workload connected with the Global War on Terror.

(TS//^(b)₍₁₎) **Intelligence Oversight Training.** (b)(1) provide intelligence oversight training (b)(1) to SSC-SD personnel. As of August 2007, (b)(1) had trained (b)(1) SSC-SD personnel (b)(1) workload, however, has caused delays in completing training for the remaining SSC-SD personnel. To ensure that SSC-SD personnel have background on intelligence oversight requirements, all (b)(1) personnel have read training material on intelligence oversight requirements. The SSC-SD is not required by DoD Directive 5240.1-R to have an intelligence oversight program; therefore, command personnel do not have the authority to provide intelligence oversight training.

DoD Wide Research and Development Facilities (U)

(TS//^(b)₍₁₎) (b)(1) has taken some steps to identify and initiate controls over (b)(1) by other research and development facilities. actions taken to date have been ineffective. (b)(1)

(b)(1)

(TS//^(b)₍₁₎) (b)(1) had initiated corrective measures related to SSC-SD. However, (b)(1) was not providing intelligence oversight to other research and development facilities (b)(1) was not focused on this issue and could not identify research and development facilities (b)(1) agreed to the following recommendations and completion dates:

- Identify research and development facilities (b)(1) by January 29, 2007;
- Establish a process to document (b)(1) these research and development facilities by February 28, 2007;

- Issue interim (b)(1) guidance to these research and development facilities by March 1, 2007;
- Implement intelligence oversight training and an intelligence oversight plan for these research and development facilities by March 30, 2007; and
- Issue standard project management guidance to (b)(1) contacts for these research and development facilities by March 1, 2007.

(TS//~~(S)~~) (b) None of these actions have been completed. (b)(1) personnel have not completely identified all the research and development facilities (b)(1). Responsibility for this action was transferred to (b)(1)

(b)(1) it plans to initiate action to complete the remaining recommended actions. (b)(1)

(b)(1) the actions will not ensure that all work done by those facilities for DoD intelligence components will be controlled in accordance with DoD Regulation 5240.1-R.

Research and Development Facilities not Included in DoD Regulation 5240.1-R (U)

(U) The DoD has not established procedures for control or oversight of U.S. persons information that may be obtained by research and development facilities. The DoD Regulation 5240.1-R does not include research and development facilities. There are no requirements for U.S. persons data, if collected by a research and development facility, to be safeguarded or reported for intelligence oversight purposes in accordance with DoD Regulation 5240.1-R.⁹

Control and Oversight of United States Persons Information (U)

(TS//~~(S)~~) (b) While the allegation of perceived mishandling of U.S. persons information at SSC-SD was not substantiated, SSC-SD had only recently received training for its staff on intelligence oversight requirements, including the handling

⁸ (U//~~(S)~~) As of July 30, 2007, this action still has not occurred.

⁹ (U) For a detailed discussion of DoD Regulation 5240.1-R, see Appendix C.

of U.S. persons information. Intelligence officials at SSC-SD told us that they had no authority to require intelligence oversight training to their staff because SSC-SD was not a "DoD intelligence component" as defined in DoD Regulation 5240.1-R.

(U//~~FOUO~~) Intelligence officials at SSC-SD also asked, "If there were intelligence oversight violations, to which entity would we report them?" The regulation does not specify how or to whom research and development facilities would report intelligence oversight violations. In November 2003, the Assistant to the Secretary of Defense for Intelligence Oversight [ATSD (IO)] visited SSC-SD. According to an official at SSC-SD, the ATSD (IO) stated that, because SSC-SD worked on projects for various components of the Intelligence Community and accepted SPAWAR (b)(1) program monies, SSC-SD was subject to intelligence oversight training requirements but not intelligence oversight reporting requirements. The ATSD (IO) stated, however, that any intelligence oversight concerns could be reported directly to the ATSD (IO).

(TS//~~(b)~~) Despite this oral guidance, other intelligence officials believe that research and development facilities such as SSC-SD are not within the parameters of DoD Regulation 5240.1-R. Officials from the NGA, and the Office of the Naval Inspector General, Intelligence/Special Access Program Oversight Division confirmed that research and development facilities like SSC-SD are not within the scope of the regulation. For example, one official at the NGA told us that, with respect to domestic imagery, intelligence oversight requirements are triggered only if NGA SPAWAR (b)(1) assets are used. Moreover, officials from the Office of the Naval Inspector General, Intelligence/Special Access Program Oversight Division stated that they had no authority to conduct intelligence oversight inspections of research and development facilities such as SSC-SD.

(TS//~~(b)~~) The only means by which senior intelligence officials at SSC-SD can require intelligence oversight training is (b)(1) [redacted] is an insufficient method to ensure SSC-SD is adequately trained in all aspects of intelligence oversight. While establishing (b)(1) [redacted] the actions will not ensure that all work done by those facilities for DoD intelligence components will be controlled in accordance with DoD Regulation 5240.1-R.

Recommendations and Management Comments (U)

~~(U//FOUO)~~ We recommend the Assistant to the Secretary of Defense for Intelligence Oversight:

1. Amend DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982, to include research and development facilities performing work for DoD intelligence components; and
2. Issue interim guidance to include research and development facilities performing work for DoD intelligence components effective until the Regulation is amended.

~~(U//FOUO)~~ **Management Comments.** The Acting Assistant to the Secretary of Defense for Intelligence Oversight concurred with the recommendations stating that DoD Regulation 5240.1-R will be amended and interim guidance will be issued. The definition of intelligence activities to intelligence and intelligence-related activities will be changed. Research and development facilities performing work for DoD intelligence components will be included in the definition of intelligence and intelligence-related activities.

(b)(1)

Appendix A. Scope and Methodology (U)

(U//~~FOUO~~) We reviewed documentation dating from April 2004 through August 2007 that included background information, test plans, project summaries, e-mail correspondence, intelligence oversight reports, training and security records, and project summaries. We conducted interviews with officials at the ATSD (IO), Navy IG, (b)(1) NRO, NGA, and SSC-SD. We determined that it was unnecessary to review multiple DoD research and development facilities because sufficient information was available at (b)(1) NRO and NGA regarding the need for controls at these facilities.

(U) We performed this review from January 2007 through August 2007 in accordance with generally accepted government auditing standards. We relied on information from (b)(1)

(U) **Use of Computer-Processed Data.** We did not use computer-processed data to perform this review.

(U) **Government Accountability Office High-Risk Area.** The Government Accountability Office has identified several high-risk areas in DoD. This report provides coverage of the Protecting the Federal Government's Information Systems and the Nation's Critical Infrastructures high-risk area.

Prior Coverage (U)

(U) During the last 5 years, (b)(1)
The NRO Office of Inspector General issued a memorandum in response to a referral (b)(1) concerning allegations of unauthorized (b)(1) by NRO.

(b)(1)

(b)(1)

Appendix B. Intelligence Community Whistleblower Protection Act (U)

(U//~~FOUO~~) The Intelligence Community Whistleblower Protection Act (ICWPA), part of the Intelligence Authorization Act for Fiscal Year 1998, amended the Inspector General Act of 1978 to provide a means by which employees (civilian and military) of, or employees of contractors to, the four DoD intelligence agencies (the Defense Intelligence Agency, NGA, NRO, and (b)(1)) may report to the Congress classified information about alleged wrongdoing of "urgent concern." Agency or contractor employees, who intended to submit to Congress a complaint or information "with respect to an urgent concern," could contact the IG, DoD. Under the provisions of the Fiscal Year 1998 Intelligence Authorization Act, if the IG, DoD, determined that the complaint or information appeared credible, the IG, DoD, would transmit the complaint or information to the Secretary of Defense within 14 calendar days after receipt from the employee or contractor. The Secretary could add comments, but was required to forward the transmittal to the Intelligence Committees of Congress within 7 calendar days after receipt from the IG, DoD.

(U//~~FOUO~~) The Intelligence Authorization Act for Fiscal Year 2002, enacted on December 28, 2001, amended the ICWPA process so that now, following the IG, DoD, determination regarding credibility, all complaints or information must be forwarded to the Secretary of Defense together with the determination. All other provisions of the ICWPA remain in effect.

(U//~~FOUO~~) The ICWPA requires that the IG, DoD inform the agency or contractor employee of each action taken during the notification process within three days of the action. The Act provides that the employee may contact the Intelligence Committees of Congress directly, if the IG, DoD, does not forward the complaint or information to the Secretary of Defense or the employee believes that the IG, DoD, did not do so accurately. Before doing so, however, the employee must obtain and follow direction from the Secretary of Defense, through the IG, DoD, on how to make such contacts in accordance with appropriate security practices.

Appendix C. DoD Regulation 5240.1-R, “Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons,” December 1982 (U)

(U) DoD Regulation 5240.1-R governs the manner in which DoD intelligence components conduct intelligence activities, including research and development of electronic equipment, and oversight of intelligence activities. Procedure 1, Applicability and Scope, states that the regulation applies only to “DoD intelligence components, as defined in the Definitions Section.” The definition does not include research and development facilities.¹⁰ Therefore, any research and development facilities that may be performing work for DoD intelligence components that may involve collection of U.S. persons information are not specifically subject to the collection, retention, dissemination, or oversight requirements of DoD Regulation 5240.1-R.

(U) Each procedure contained in DoD Regulation 5240.1-R governs the manner in which DoD intelligence components conduct intelligence activities concerning U.S. persons.

- Procedure 2, Collection of Information about U.S. persons; Procedure 3, Retention of Information about U.S. persons; and Procedure 4, Dissemination of Information about U.S. persons, provide the sole authority by which DoD Intelligence Components may collect, retain and disseminate information concerning U.S. persons.
- Procedure 5, Electronic Surveillance; Procedure 6, Concealed Monitoring; Procedure 7, Physical Searches; Procedure 8, Searches and Examination of Mail; Procedure 9, Physical Surveillance; and Procedure 10, Undisclosed Participation in Organizations, set forth

¹⁰ (U) DoD intelligence components are defined as the following organizations: the National Security Agency/Central Security Service; the Defense Intelligence Agency; the offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; the Assistant Chief of Staff for Intelligence, Army General Staff; the Office of Naval Intelligence; the Assistant Chief of Staff, Intelligence, U. S. Air Force; the Army Intelligence and Security Command; the Naval Intelligence Command; the Naval Security Group Command; the Director of Intelligence, U.S. Marine Corps; the Air Force Intelligence Service; the Electronic Security Command, U.S. Air Force; the counterintelligence elements of the Naval Investigative Service; the counterintelligence elements of the Air Force Office of Special Investigations; the 650th Military Intelligence Group, SHAPE; other organizations, staffs, and offices, when used for foreign intelligence or counterintelligence activities to which part 2 of E.O. 12333, applies, provided that the heads of such organizations, staffs, and offices shall not be considered as heads of DoD intelligence components for purposes of this regulation.

guidelines regarding the use of certain collection techniques by DoD Intelligence Components to obtain information for foreign intelligence and counterintelligence purposes.

- Procedure 11, Contracting for Goods and Services; Procedure 12, Provision of Assistance to Law Enforcement Authorities; Procedure 13, Experimentation on Human Subjects for Intelligence Purposes, govern other aspects of DoD intelligence activities. Procedure 14, Employee Conduct and Procedure 15, Identifying, Investigating, and Reporting Questionable Activities, provide for oversight of DoD intelligence activities.

Appendix D. Report Distribution (U)

(U)

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense for Intelligence
Assistant to the Secretary of Defense for Intelligence Oversight

Department of the Army

Deputy Chief of Staff for Intelligence
Inspector General

Department of the Navy

Director, Naval Intelligence
Inspector General
Director, Marine Corps Intelligence

Department of the Air Force

Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance
Inspector General

Other Defense Organizations

Director, National Security Agency/Central Security Service
Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Geospatial-Intelligence Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organization

Director of National Intelligence
Inspector General, Office of the Director of National Intelligence

Congressional Committees and Subcommittees

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 Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Oversight and Government Reform
House Permanent Select Committee on Intelligence

THIS PAGE INTENTIONALLY LEFT BLANK (U)

Appendix E. Report of Investigation of Alleged Reprisal (b)(1)

FOR OFFICIAL USE ONLY
Report No. HL102317

Inspector General

United States
Department of Defense



- FINAL -

Report of Investigation of Alleged Reprisal (b)(1)
(b)(1)

Warning
The enclosed document(s) is (are) the property of the Department of Defense, Office of Inspector General. It is to be controlled, stored, handled, transmitted, disseminated, and disposed of in accordance with the Department of Defense Information Security Manual (DOD ISM) and the Department of Defense Security Manual (DDSM). It is to be protected from unauthorized disclosure and its use is limited to the purposes for which it was prepared and the Department of Defense Office of Inspector General.

FOR OFFICIAL USE ONLY



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

SEP 26 2007

MEMORANDUM FOR (b)(1)

SUBJECT: Investigation under 5 U.S.C. § 2302(a)(2)

We recently completed our investigation into allegations that (b)(1) and (b)(1) reprimed against (b)(1) by:

- Denying promotion, awards and time off;
- Denying reassignment;
- Failure to provide interim evaluation;
- Mistreatment by management (official counseling);
- Lowered performance appraisal;

-and-

- Forced resignation.

Attached we provide you with our Report of Investigation non-substantiating the allegations. (b)(1) provided clear and convincing evidence that the personnel action would have occurred absent the protected disclosures (b)(6), (b)(7)(C) made.

If you have any questions, please contact me or (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)

Donald M. Horstman
Assistant Inspector General for
Administrative Investigations

Attachment:
As stated

(b)(6), (b)(7)(C)

INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

- FINAL -
REPORT OF INVESTIGATION

(b)(1) OFFICIALS TOOK NO ADVERSE PERSONNEL ACTION AGAINST
THE COMPLAINANT IN REPRISAL FOR PROTECTED DISCLOSURES.

1. INTRODUCTION AND SUMMARY

The Complainant (b) (6) (b) (7)(C) alleges reprisal by his first and second line supervisors at (b)(1) (b)(1) also known as the (b)(1) filed an Intelligence Community Whistleblower Protection Act (ICWPA) complaint with the Deputy Inspector General for Intelligence (DoDIG) on December 18, 2006 (H1.# 102317). The Deputy Inspector General for Intelligence initiated an investigation and requested subject matter expertise from the Directorate, Civilian Reprisal Investigations (CRI).

Prior to filing his ICWPA complaint with DoDIG, (b) (6) (b) (b) alleged reprisal by his first and second line supervisors (b)(1). He alleged denial of promotion and mistreatment by management. CRI conducted oversight for this part of (b)(1) investigation. After the completion of (b)(1) investigation, (b) (6) (b) filed the ICPWA complaint with DoDIG alleging not only denial of promotion and mistreatment by management, but also denial of awards and time off, no interim evaluation, and forced resignation. Therefore, CRI initiated their own investigation to address the remaining allegations. As an act of oversight, we reviewed the results of the (b)(1) investigation, concur and incorporated (b)(1) results into this Report of Investigation.

The Complainant alleges six (6) acts of reprisal:

- Denial of promotion, awards, and time off by (b) (6) (b) (7)
- Denial of reassignment by (b) (6) (b) (7)(C)
- No interim evaluation by (b) (6)
- Mistreatment by management by (b) (6) (official counseling);
- Lowered performance appraisal;

—and—

- Forced resignation.

The disclosures were made upon (b) (6) (b) reasonable belief that violations of law occurred at the Space and Naval Warfare Systems Command (SPAWAR) San Diego, California. The violations of law that (b) (6) (b) reported on, are of a classified nature

~~UNCLASSIFIED//NOFORN~~

and are documented by the Deputy Inspector General for Intelligence under separate cover.

(b) (6), (b) (7) had standing to file a complaint with the Department of Defense Hotline under the Inspector General Act of 1978 ("IG Act"), as amended. He requested filing status under the Intelligence Community Whistleblower Protection Act of 1998 ("ICWPA"). The allegations were therefore investigated pursuant to both Section 7 of the IG Act and the ICWPA. In addition, when (b)(1) (b)(1) previously requested oversight by the Department of Defense's Office of the Inspector General, we opened an oversight investigation under IG Act. Both statutes provide authority for this investigation. (p)

This Report of Investigation ("ROI") is based on an examination of documents and testimony to determine if a nexus existed between (b) (6), (b) (7)(C) protected disclosures and the alleged adverse actions by (b)(1)

(b) (6), (b) (7) presented, and this investigation has collected, evidence proving that the denial of promotion awards and time off, denial of reassignment, denial of interim evaluation, mistreatment by management, lowered performance appraisal, and forced resignation were adverse actions possibly connected to one or more of his protected disclosures. Because a prima facie case was presented, the burden shifted to (b)(1) to demonstrate by clear and convincing evidence that the prohibited personnel actions would have occurred absent the protected disclosure. (D4).

After review of relevant testimony and documents, DoDIG finds that (b)(1) officials did not reprise against the Complainant for his protected disclosures.

(b) (6), (b) (7) made three protected disclosures. He made a disclosure to (b)(1) (b)(1) on June 17, 2005 (disclosure 1), (b)(1) on July 25, 2005 (disclosure 2), and (b)(1) on September 25, 2005 (disclosure 3). (M) On December 18, 2006, (b) (6), (b) (7) filed an Intelligence Community Whistleblower Protection Act (ICWPA) complaint with the Department of Defense Deputy Inspector General for Intelligence. (M08)

Specifically, we determined that two alleged adverse actions did not warrant further investigation. First, (b) (6), (b) (7) was not reprised against when he received a lowered performance appraisal in 2003. (M09) The lowered performance appraisal in 2003 cannot be considered an adverse action resulting from a protected disclosure, because the

¹ Complainant made numerous disclosures to (b)(1) his chain-of-command, and the Department of Defense Inspector General during this period. We do not address these disclosures individually because we find that addressing the individual disclosures would not affect the outcome of the case. For simplicity purposes disclosures made to (b)(1) and his chain-of-command were counted as one disclosure each.

ORIGINATOR NAME OR IDENTIFYING ORG

(b)(1)

alleged personnel action occurred approximately two years prior to any protected disclosure.

Second, (b)(6) (b)(7)(C) allegation that he was forced to resign does not qualify as an adverse action, because (b)(6) (b)(7) did not actually resign his position (b)(1) instead he transferred to another department (b)(1) (b)(6) (b)(7)(C) "resignation" was, at best, an allegation of constructive reassignment. As his new duties are within fifty (50) miles of his former duties and pose no threat to his future prospects within (b)(1) the transfer is not considered an adverse action (b)(1).

Therefore, for purposes of this investigation we are only considering disclosures two and three because these two protected disclosures provide both certainty as to what was stated to whom, and fall within a time period sufficient to aid in the analysis of this investigation.

The complainant alleges the following personnel practices were taken in reprisal:

- Denial of promotion, awards, and time off;
- Denial of reassignment;
- Denial of interim evaluation;

--and--

- Mistreatment by management (official counseling).

We determined that (b)(1) officials had actual knowledge of one (D11) or more of the disclosures at the time they took the adverse personnel actions as (b)(6) (b)(7) was a source of an Inspector General special study and also a vocal critic of the issues at SPAWAR. We further find that the denial of promotion, awards, and time off, denial of reassignment, and denial of interim evaluation occurred within a thirteen (13) month period such that a reasonable person might conclude that the disclosure was a contributing factor in (b)(1) decision. (M012)

Further, it should be noted that for the allegation concerning denial of reassignment and denial of an interim evaluation, (b)(1) failed to follow its own regulations.

II. BACKGROUND

(b)(1)

CONFIDENTIAL - NO FORN DISSEM

(b)(1)

(b)(1) In his role as (b)(1) (b)(6) (b)(7) was assigned to (b)(1) (b)(1) (b)(6) (b)(7) (b)(1) (b)(1)

In March/April 2004, (b)(6) (b)(7) received numerous requests for assistance from SPAWAR personnel. (b)(6) (b)(7) spoke to his then-supervisor, (b)(6) (b)(7)(C) and requested to go on temporary duty (TDY) to determine SPAWAR's issues and requirements. (b)(6) (b)(7)(C) TDY initially was disapproved due to non-availability of funds. However, (b)(6) (b)(7) continued to receive requests for assistance from SPAWAR, and so he continued to push for approval of his TDY. Finally, (b)(6) (b)(7) informed his then-supervisor that SPAWAR planned to send a P4 (personal for) message to (b)(1) requesting assistance. Based on this information, (b)(6) (b)(7)(C) TDY was approved and he proceeded to SPAWAR in September 2004.

During (b)(6) (b)(7)(C) visit to SPAWAR he identified an immediate need for a Memorandum of Agreement between SPAWAR and (b)(1) as well as other issues which are classified (S). For approximately one year following the visit (b)(6) (b)(7) worked to establish a Memorandum of Agreement, continuously encountering obstacles in obtaining final approval. (b)(6) (b)(7)(C) first-line supervisor encouraged him to continue solving SPAWAR's issues, in opposition to (b)(6) (b)(7)(C) second-level supervisor. (b)(6) (b)(7)(C) was not in favor of it. According to testimony by (b)(6) (b)(7) and (b)(6) (b)(7)(C) "did not like to make waves" and told (b)(6) (b)(7)(C) to "stay in his lane."

Finally, (b)(6) (b)(7) turned to (b)(6) (b)(7)(C) who was (b)(1) (b)(1) After a meeting with (b)(6) (b)(7) on July 25, 2005, (b)(6) (b)(7) was tasked to assemble a team of inspectors, develop, and accomplish a full (b)(1) assessment of SPAWAR (b)(1).

In August 2005, (b)(6) (b)(7) applied for a position (b)(1) (b)(1) office and was selected. (b)(6) (b)(7) However, (b)(6) (b)(7) supervisor, (b)(6) (b)(7)(C) informed him that he was going to put a 180-day hold on (b)(6) (b)(7) s reassignment because of the ongoing (b)(1) assessment of SPAWAR. On September 12, 2005, (b)(6) (b)(7) sent an email to (b)(6) (b)(7) (b)(1) and informed her that he could not release (b)(6) (b)(7) and that he was going to put a 180-day hold on him (b)(1) because (b)(6) (b)(7) was involved in a critical undertaking with regard to fixing a problem that he had uncovered. Because (b)(1) vacancy needed to be filled, (b)(1) management decided to select another candidate. Later, (b)(6) (b)(7) contacted his Human Resources office and was informed that there was no provision for a 180-day hold and that, at most, his supervisor could hold

~~TOP SECRET~~

him for 120 days. Anything above that had to be approved on a case by case basis through the Director, Human Resources.

Following the July 25, 2005 meeting between (b)(6), (b)(7)(C) and (b)(6), (b)(7)(C) (b)(1) (b)(1) (b)(1) and detailed SPAWAR's issues. Because (b)(6), (b)(7) was (b)(1) had discovered SPAWAR's problems he was also contacted and met with (b)(1) approximately on September 28, 2005 (p22).

Attempting to determine the extent of the problem with other Research and Development Laboratories, the Deputy Inspector General for Intelligence Oversight, (b)(6), (b)(7)(C) tasked a special study on October 7, 2005, pertaining to Research and Development Laboratories' (b)(1) (b)(6), (b)(7) also asked (b)(6), (b)(7) to provide a written unabridged historical account from the time SPAWAR's issues first surfaced (p23).

On October 14, 2005, (b)(6), (b)(7) responded to (b)(6), (b)(7) request for a chronology and documentation on the SPAWAR issues and sent it to his supervisor (b)(6), (b)(7)(C) who forwarded it to (b)(6), (b)(7) stated in the email to (b)(6), (b)(7) that at a minimum the chronology needed to be cleaned up and made more understandable (p23).

After assembling a team of inspectors, (b)(6), (b)(7) proceeded to SPAWAR on October 23-28, 2005. Upon (b)(6), (b)(7)(C) return (b)(1) he wrote a trip report of SPAWAR's shortcomings (p26).

On November 1, 2005, (b)(6), (b)(7)(C) Deputy Inspector General for Intelligence Oversight, contacted (b)(6), (b)(7) about the status of the chronology. (b)(6), (b)(7) responded that his Division had requested review of his response to her organization and were still in the process of doing the review. However, he forwarded a copy of his response directly to her in the interest of complying with her request. Meanwhile, (b)(6), (b)(7) forwarded the SPAWAR chronology to (b)(6), (b)(7) informing him that the IG was eagerly awaiting it but that she wanted his review and approval before submitting it to the IG. (b)(6), (b)(7) made some minor changes.

On November 4, 2005, (b)(6), (b)(7) briefed (b)(6), (b)(7) on his findings at SPAWAR. (b)(6), (b)(7) instructed (b)(6), (b)(7) to not actively engage the Research and Development Laboratories, but to have the Labs come to (b)(1) for assistance. (b)(6), (b)(7) and his management were confused about (b)(6), (b)(7)(C) instructions and so (b)(6), (b)(7) asked the (b)(1) (b)(6), (b)(7)(C) (b)(1) to speak with (b)(6), (b)(7) to obtain clarification (p27).

On February 15, 2006, (b)(6), (b)(7) received an email from (b)(6), (b)(7)(C) (b)(1) informing him that she and (b)(6), (b)(7) had a meeting with (b)(1) and that (b)(6), (b)(7) would be able to stop activities regarding the Labs and start concentrating on his (b)(1) (b)(1) (MO28) After (b)(6), (b)(7) spoke to (b)(6), (b)(7)

~~TOP SECRET~~

(b)(6) (b)(7)(C) about the (b)(1) meeting. (b)(6) (b)(7)(C) sent an email on February 23, 2006, to several individuals to inform them that per direction from (b)(1) (b)(6) (b)(7)(C) would not be the focal point for outreach to the other Research and Development Laboratories; that the entire decision on outreach to Research and Development Laboratories was now controlled by (b)(1) (b)(6) (b)(7)(C) became upset about the email, because she felt that the email did not meet her guidance and ordered (b)(6) (b)(7)(C) to rescind the email, which he did the following day.

On April 13, 2006 (b)(6) (b)(7)(C) received an email from (b)(6) (b)(7)(C) inquiring about the visit request status for an individual from SPAWAR, San Diego. (b)(6) (b)(7)(C) responded and declared that he would like to engage; however, according to management, until (b)(1) study was completed, no new interaction with SPAWAR was to be initiated. He also claimed that (b)(1) had coordinated their direction with the (b)(1) (b)(6) (b)(7)(C). That afternoon, (b)(6) (b)(7)(C) (b)(1) (b)(1) in coordination with (b)(1) (b)(6) (b)(7)(C) sent an email to (b)(6) (b)(7)(C) asserting that (b)(1) (b)(1) knew of no legal or policy reasons that required (b)(1) to reduce or restrict (b)(1) interaction with SPAWAR (b)(1).

(b)(6) (b)(7)(C) was called into (b)(6) (b)(7)(C) office for an "official" counseling (b)(1). (b)(6) (b)(7)(C) verbally counseled (b)(6) (b)(7)(C) that he had overstepped his authority and to "cease and desist." (b)(6) (b)(7)(C) denied any intent to convey the wrong message and subsequently (b)(6) (b)(7)(C) decided not to formalize the counseling (b)(1).

On April 18, 2006 (b)(6) (b)(7)(C) sent an email to the (b)(1) (b)(1) claiming retaliation in response to his involvement with the October 7, 2005 (b)(1) directed special study. (b)(6) (b)(7)(C) alleged that he was told that he was not going to be promoted because of the SPAWAR issue and his involvement, that he was formally counseled, that a 180-day hold had been placed on him in the fall of 2005 because his efforts were too important for him to leave, and that (b)(1) tried to modify documents that he had submitted (b)(1) (b)(1).

On May 3, 2006, (b)(6) (b)(7)(C) requested reassignment to (b)(1) (b)(1) which was approved on May 15, 2006.

After (b)(6) (b)(7)(C) is reassignment to (b)(1) in June 2006 (b)(6) (b)(7)(C) unsuccessfully tried to obtain an interim (b)(1) (b)(1) for his performance as (b)(1) (b)(1) (b)(1) (b)(1) claims that he repeatedly contacted his former supervisor (b)(6) (b)(7)(C) without success (b)(6) (b)(7)(C) new supervisor, (b)(6) (b)(7)(C) (b)(6) (b)(7)(C) also tried to assist (b)(6) (b)(7)(C) in obtaining an interim (b)(1) without (b)(1).

² (b)(6) (b)(7)(C) was assigned by (b)(1) to conduct an assessment of conditions at SPAWAR. His responsibility did not include management of the response to the conditions he reported upon. By following up on matters beyond the scope of his assignment, he exceeded his job responsibilities and eventually became a source for both (b)(1) (b)(1) and the Inspector General of the U.S. Department of Defense. For this reason, we found his communications to meet the requirement that they not be in the normal course of one's duties.

~~TOP SECRET~~

successes). During CRI's interview with (b)(6) (b)(7)(C) he denied having ever received a request to provide an interim (b)(1)

On December 18, 2006, (b)(6) (b)(7) contacted the Department of Defense Inspector General and filed a complaint under the Intelligence Community Whistleblower Protection Act (ICWPA).

(b)(1) conducted an investigation, after coordination with the Deputy Inspector General for Intelligence and the Civilian Reprisal Investigations Directorate (CRI), Department of Defense. On May 3, 2007, (b)(1) produced a report and submitted the report to DoDIG, CRI for oversight. (b)(1) report substantiated no reprisal. DoDIG, CRI conducted the oversight review and principally concurred with (b)(1) findings pertaining to the denial of promotion and mistreatment by management (official counseling). However, because (b)(6) (b)(7) alleged several additional adverse actions in his ICWPA complaint of December 2006 which had not been part of (b)(1) DoDIG, CRI continued the investigation to address the remaining allegations. The remaining allegations consisted of denial of reassignment, denial of promotion, awards, and time off, denial of interim evaluation, and forced resignation.

III. SCOPE

We interviewed four witnesses, including the Complainant. We also reviewed classified and unclassified documentation provided by (b)(6) (b)(7) and (b)(1) related to the matters under investigation.

IV. FINDINGS AND ANALYSIS

Standards

Title 5, United States Code, Appx., §§ 7 (a) and (c).

This section permits an employee to file a whistleblower complaint with the DoDIG.

Title 5, United States Code, Section 2301 and 2302, "Prohibited Personnel Practices," (5 U.S.C. Sections 2301 and 2302).

These sections prohibit an agency from taking an adverse personnel action against a civilian employee hired under Title 5 (appropriated fund) for making a protected disclosure. "Protected disclosures" include information that the civilian employee reasonably believes evidences, among other things, a violation of law, rule, or regulation; gross mismanagement; gross waste of funds; or an abuse of authority.

Title 5, United States Code, Section 2302 (a)(2)(A)(i) through (xi).

~~UNCLASSIFIED//TOP OFFICIAL USE ONLY~~

Title 5, Section 2302 (a)(2)(A)(i) through (xi) defines those personnel actions which, if taken, recommended, or approved, in reprisal for a protected disclosure, constitute "prohibited personnel practices."

These personnel actions include disciplinary or corrective action; a detail, transfer or reassignment; a performance evaluation; a decision concerning pay, benefits, or award; or any other significant change in duties, responsibilities, or working conditions.

Title 5, Code of Federal Regulations, Section 1209.7, "Burden of Proof."

A complainant asserting reprisal for whistleblowing activity must first establish by a preponderance of the evidence that: 1) he made a protected disclosure; and 2) that such disclosure was a contributing factor in an adverse personnel action that he challenges. A complainant successfully demonstrates, *prima facie*, reprisal when he establishes, by a preponderance of the evidence, that he made a protected disclosure and such disclosure was a contributing factor in an adverse personnel action.

Thereafter, the burden of persuasion shifts to the agency to show by "clear and convincing" evidence that it would have taken the personnel action in the absence of the protected disclosure.

Title 5, Code of Federal Regulations, Section 1209.4, "Definitions."

A "contributing factor" means any disclosure that affects an agency's decision to threaten, propose, take, or not take, a personnel action with respect to the individual making the disclosure.

"Clear and convincing evidence" is that measure or degree of proof that produces in the mind of the fact finder a firm belief as to the allegations sought to be established. It is a higher standard than "preponderance of the evidence."

Executive Order 12674 (Apr. 12, 1989) (as mod. by E.O. 12731).

Employees of the Department of Defense are required to report "waste, fraud, abuse and corruption." This Order is obligatory, not optional. Civilian Appropriated-Fund Personnel may file a complaint of reprisal with the Defense Hotline under Section 7 of the Inspector General Act of 1978. Appendix 3, Title 5, United States Code.

The Intelligence Community Whistleblower Protection Act of 1998, Pub. L. 105-272, Title VII, 112 Stat. 2413 (1998).

Authorizes any employee or contractor to an executive agency, or element or unit to have as its principal function the conduct of foreign intelligence or counterintelligence activities, who intends to report to Congress a complaint or information with respect to an

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

urgent concern may report the complaint or information to the appropriate Inspector General under this Act.

E.O. 12333, United States Intelligence Activities (Dec. 4, 1981), as amended.

Activities conducted under E.O. 12333, provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats.

(b)(1)

Interim Evaluations (to include summary information and numerical ratings) shall be completed to document performance during the cycle when the employee has been performing under a plan for at least 90 days and if the rater is reassigned; an employee is detailed or reassigned; or there is significant change in the employee's duties.

(b)(1)

This policy reduces the amount of time that an employee may be held to 90 days; allows for holds over 90 days with (b)(1) approval.

Facts

(b)(6), (b)(7) made three protected disclosures. The disclosures transmitted (b)(6), (b)(7)(C) reasonable belief that violations of law occurred at the Space and Naval Warfare Systems Command (SPAWAR). The disclosures he made were to (b)(6), (b)(7)(C) b(1) on June 17, 2005 (disclosure 1); (b)(6), (b)(7), b(1) on July 25, 2005 (disclosure 2); (b)(1) on September 25, 2005 (disclosure 3)³. On December 18, 2006 (b)(6), (b)(7) filed an Intelligence Community Whistleblower Protection Act (ICWPA) complaint with the Deputy Inspector General for Intelligence.

The time interval between (b)(6), (b)(7)(C) first disclosure to his last alleged reprisal action, specifically the denial of an interim (b) was approximately thirteen (13) months (04). A period of time this brief permits the inference that the protected disclosures may have been a contributing factor in the adverse personnel actions. As such, this is an acceptable interval in determining if (b)(6), (b)(7)(C) disclosures were contributing factors in the adverse actions.

³ Complainant made numerous disclosures to (b)(1) during this period. We do not address these disclosures individually because we find that the dates of the individual disclosures would not affect the outcome of the case.

~~TOP SECRET~~ (b)(1)

(b) (6), (b) (7)(C) chain-of-command had knowledge of his disclosures, because (b) (6) (b) (6), (b) (7)(C) had briefed (b) (6), (b) (7)(C) (b)(1) (b) (6), (b) (7)(C) on July 25, 2005, about the issues he found at SPAWAR, San Diego (b)(1). (b) (6), (b) (7)(C) notified (b) (6), (b) (7)(C) of his briefing (b)(1).

Discussion

a. Denial of promotion, awards, and time off by (b) (6), (b) (7)(C)

(b) (6), (b) (7)(C) allegation of denial of promotion was one of the allegations covered (b)(1) (b)(1) We reviewed (b)(1) and it demonstrated that (b) (6), (b) (7)(C) s first and second-line supervisors would have denied (b) (6), (b) (7)(C) promotion absent his disclosures. (b)(1) has provided clear and convincing evidence and we concur with the finding of no reprisal pertaining to the denial of promotion. However, (b) (6), (b) (7)(C) alleged further reprisals in his complaint to the Department of Defense Inspector General in December 2006. He alleged that not only was he denied promotion but also that he did not receive any financial or time off awards.

We reviewed the Standard Form 50s that (b) (6), (b) (7)(C) provided to us and found that he received several time-off awards. In August 2004, (b) (6), (b) (7)(C) received a group time-off award of 24 hours; in June 2005, he received an individual time-off award of 24 hours; in October 2005 he once again received a group time off award of 8 hours. So between August 2004 and October 2005, a 13-month period, he received 56 hours of time off as award for his performance.

(b) (6), (b) (7)(C) then-supervisor (b) (6), (b) (7)(C) testified that he submitted (b) (6), (b) (7)(C) name together with two other employee names to (b) (6), (b) (7)(C) for a performance award in early 2006. Only one of those employees received a performance award at that time. Performance awards are discretionary to the supervisor. Not every employee's performance is recognized. Performance recognition can range from monetary awards, time-off awards, to honorary awards. It appears, (b) (6), (b) (7)(C) immediate supervisor (b) (6), (b) (7)(C) felt that (b) (6), (b) (7)(C) deserved a performance award when he submitted (b) (6), (b) (7)(C) name to (b) (6), (b) (7)(C) however, (b) (6), (b) (7)(C) was not the final determining authority. The award for (b) (6), (b) (7)(C) was denied together with another person's award. Management has provided evidence, to a clear and convincing level, that the personnel action would have been taken absent the protected communications. There is no evidence of targeted denial against (b) (6), (b) (7)(C). Additionally, (b) (6), (b) (7)(C) received several time-off awards the previous year, two of which were after the initial disclosure. Also, approximately three or four months later (b) (6), (b) (7)(C) was reassigned to another position based on his own request, upon which time he received (b)(1) (b)(1) which could be considered an honorary award for his service (b)(1).

When reviewing the agency actions for evidence that (b)(1) would have not given (b) (6), (b) (7)(C) the specific performance award absent his disclosures, we were

persuaded by the granting of two time-off awards and an honorary award to (b)(6) (b)(7) even after his disclosure.

b. Denial of reassignment by (b)(6) (b)(7)

In August 2005, (b)(6) (b)(7) applied for a position as (b)(1) and was selected. When (b)(6) (b)(7) asked for a release date, his supervisor, (b)(6) (b)(7)(C) informed him that he was going to put a 180-day hold on his reassignment. (b)(6) (b)(7) based this decision on the ongoing (b)(1) and that (b)(6) (b)(7) was instrumental in resolving the issues with SPAWAR. On September 12, 2005, (b)(6) (b)(7) sent an email to (b)(6) (b)(7)(C) (b)(1) and informed her that he could not release (b)(6) (b)(7) and that he was going to put a 180-day hold on him (b)(6) (b)(7) because (b)(6) (b)(7) was involved in a critical undertaking with regard to fixing a problem that he had uncovered. Because (b)(1) vacancy needed to be filled, (b)(1) management decided to select another candidate. Later, (b)(6) (b)(7) contacted his Human Resources office and was informed that there was no 180-day hold policy and that, at most, his supervisor could hold him for 120 days. Anything above that had to be approved on a case by case basis through the (b)(1)

(b)(1) dated November 2002 reduces the amount of time that an employee may be held to 90 days. However, it allows for holds over 90 days with (b)(1) approval.

When questioned if (b)(6) (b)(7) took steps to officially request the 180-day hold from Human Resources, he admitted to not having done so (b)(6).

One could therefore conclude that (b)(6) (b)(7)(C) denial of reassignment could be reprisal were it not for the fact that (b)(6) (b)(7) based his statement on mission requirement. Additionally, (b)(6) (b)(7) sent an email to (b)(6) (b)(7)(C) stating that he would understand if (b)(1) wanted to put a hold on him. He was sure something else would open up down the road. It appeared that he even went as far as suggesting what the consequences were if (b)(1) did not put a hold on him and that (b)(1) would be forced to select another employee if there was a hold on him (b)(6).

When reviewing (b)(1) actions for the firm belief that (b)(1) would have denied (b)(6) (b)(7)(C) reassignment absent his disclosures, we point to the fact that (b)(6) (b)(7) had no personal motive to reprise against (b)(6) (b)(7). In fact, (b)(6) (b)(7) had encouraged (b)(6) (b)(7) to solve SPAWAR's issues and the decision to retain (b)(6) (b)(7) was based solely on mission accomplishment. (M49)

Evidence developed during the investigation accordingly proved to a clear and convincing standard that the personnel action would have been taken absent the protected disclosure.

~~UNCLASSIFIED FOR ORIGINAL USE ONLY~~

c. No interim evaluation by (b)(6), (b)(7)

On May 3, 2006, (b)(6), (b)(7) requested a reassignment to (b)(1) which was approved on May 15, 2006. After (b)(6), (b)(7)(C) reassignment in June 2006 he attempted to obtain an interim (b)(1) for his performance as (b)(1) (b)(6), (b)(7) sent an email to (b)(6), (b)(7) without success. (b)(6), (b)(7)(C) new supervisor (b)(6), (b)(7) also tried to obtain an interim (b)(1) without success. (b)(6), (b)(7) testified that the failure to have an interim (b)(1) diminished his chances of being selected for the 2006 promotion cycle.

During our interview with (b)(6), (b)(7) he denied having ever received a request to provide an interim (b)(1).

It cannot be determined why (b)(6), (b)(7) did not respond to (b)(6), (b)(7)(C) request for the evaluation. The possibility exists that (b)(6), (b)(7)(C) simply overlooked (b)(6), (b)(7) and (b)(6), (b)(7)(C) request because (b)(6), (b)(7)(C) stated during our interview that he was reassigned from (b)(1) on August 9, 2006. This was verified through (b)(6), (b)(7) personnel records.

(b)(6), (b)(7) stated to us that he contacted several different individuals, primarily (b)(1) with his request for interim (b)(1) (b)(6), (b)(7) no longer at (b)(1) (b)(6), (b)(7)(C) was also unable to recall any specific names since he had taken a different position as well and no longer had access to any of his prior electronic mail (email). (b)(6), (b)(7)

(b)(6), (b)(7)(C) was questioned on July 31, 2007 regarding the missing interim (b)(1) and (b)(6), (b)(7)(C) prospects for promotion. (b)(6), (b)(7)(C) stated that he did not believe that it diminished (b)(6), (b)(7)(C) chance for promotion for 2006. He acknowledged that this particular year (b)(1) had six allocations for promotion and that covered (b)(1) Many individuals had the same (b)(1) as (b)(6), (b)(7) and were also eligible to be promoted. He stated that simply not every one could get promoted. (b)(6), (b)(7) was a hard worker and he evaluated him based on his performance. (b)(6), (b)(7)(C) felt that a missing interim (b)(1) had no more and no less effect on (b)(6), (b)(7)(C) promotion. (b)(6), (b)(7)

Failure to provide an interim evaluation violates (b)(1) own policy(s); however, we do not see motive in (b)(6), (b)(7)(C) failure to provide an interim (b)(1) so as to constitute reprisal in response to (b)(6), (b)(7)(C) protected disclosures.

Evidence developed during the investigation proved to a clear and convincing standard that the personnel action would have been taken absent the protected disclosure.

~~TOP SECRET~~

d. Mistreatment by management (official counseling by (b)(6), (b)(7)(C))

(b)(6), (b)(7)(C) allegation of mistreatment by management (official counseling) was one of the allegations covered by (b)(1) report is classified Secret. We (MSJ) reviewed (b)(1) and it demonstrated by clear and convincing evidence that (b)(6), (b)(7)(C) supervisor would have counseled (b)(6), (b)(7)(C) regardless of his disclosures. Therefore, (b)(1) has established clear and convincing evidence and we concur with the finding of no reprisal pertaining to alleged mistreatment by management (official counseling).

V. CONCLUSIONS

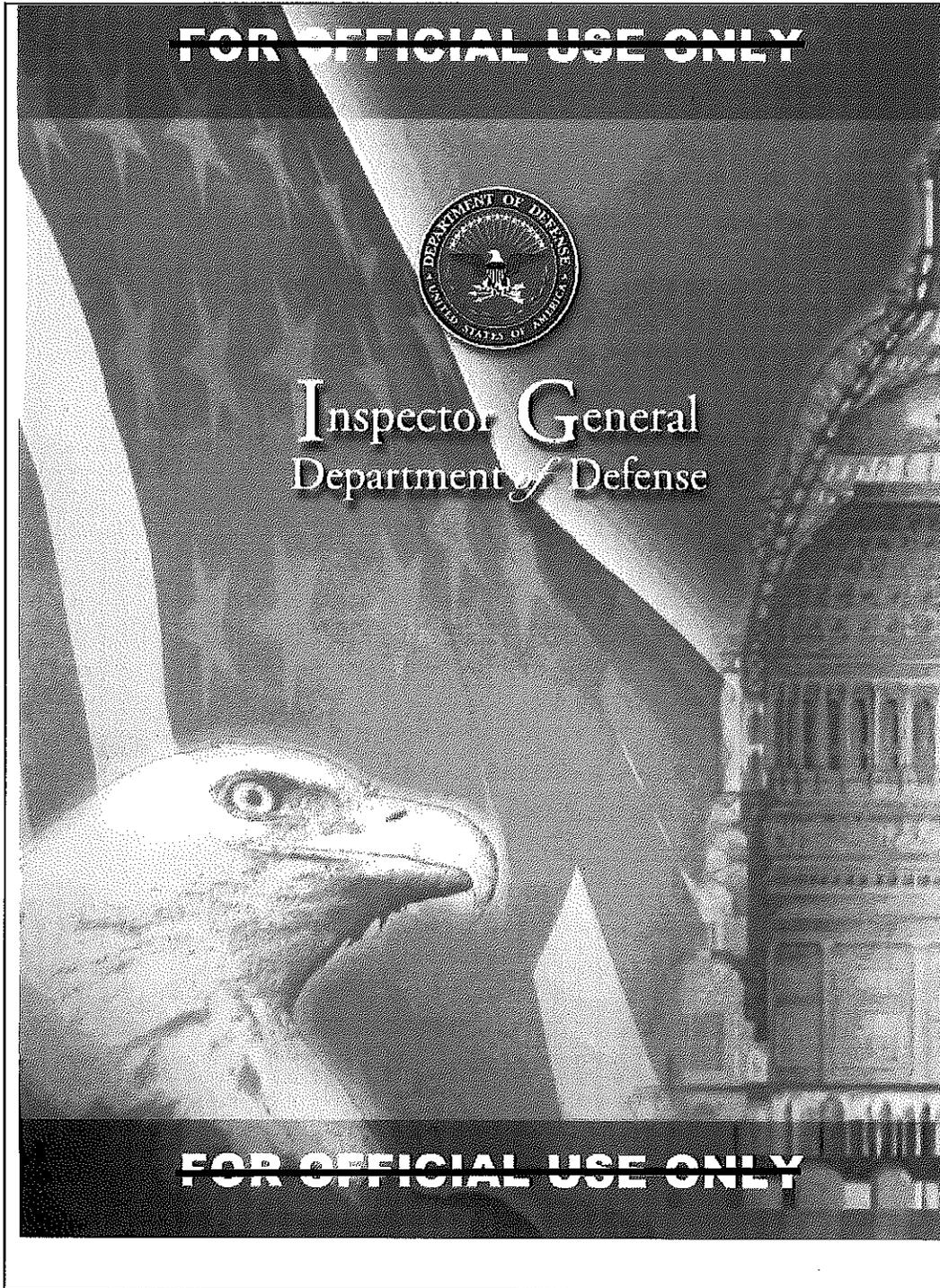
The evidence provided by management demonstrated by clear and convincing evidence that (b)(6), (b)(7) was not reprisal against when he was denied promotion, awards, and time off; denied reassignment; denied an interim evaluation; and when he was officially counseled by management. These actions would have occurred absent his disclosures.

Findings of the Investigation by the Deputy Inspector General for Intelligence pertaining to (b)(6), (b)(7)(C) allegation pertaining to SPAWAR's violations of law will be provided under separate cover by the Deputy Inspector General for Intelligence.

VI. RECOMMENDATION

We recommend that that the (b)(1) review the administrative failures addressed in this report, namely, the failure to follow procedures outlined in (b)(1) Reassignment Policy and the failure to follow (b)(1) pertaining to Interim Evaluations.

UNCLASSIFIED//FOR OFFICIAL USE ONLY



Assistant to the Secretary of Defense for Intelligence Oversight Comments (U)



INTELLIGENCE
OVERSIGHT

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

ASSISTANT TO THE SECRETARY OF DEFENSE
7200 DEFENSE PENTAGON
WASHINGTON, DC 20301-7200

September 10, 2007

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Comments on Draft Report on Review of Access to U.S. Persons Data by the Space and Naval Warfare Systems Command (Project No. D2007-DINTEL-0106) (U)

(U//~~FOUO~~) Thank you for the opportunity to comment on the draft report. We have reviewed the subject draft as requested and concur with the two recommendations regarding research and development facilities performing work for DoD intelligence components.

(U//~~FOUO~~) Specifically, upon publication of the final report, we will amend DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982, to include research and development facilities performing work for DoD intelligence components as recommended. We will also issue interim guidance on this matter to be effective until the regulation is amended.

(U//~~FOUO~~) In the interim guidance and in the revision to DoD 5240.1-R, we intend to change the definition of "intelligence activities" to "intelligence and intelligence-related activities." Research and development facilities performing work for DoD intelligence components will be included in the definition of "intelligence and intelligence-related activities."

William Dugan
Acting

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

1



THIS PAGE IS INTENTIONALLY LEFT BLANK (U)

(U)

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

(b) (6) (b) (7)(C)

(b) (6) (b) (7)(C)

TOP SECRET

(b)(1)



Inspector General Department of Defense

TOP SECRET

(b)(1)