



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

February 23, 2018
Ref: FOIA-2016-00016

SENT VIA EMAIL TO: saftergood@fas.org

Mr. Steven Aftergood
Federation of American Scientists
1725 DeSales Street NW, Suite 600
Washington, DC 20036

Dear Mr. Aftergood:

This is in response to your October 7, 2015, Freedom of Information Act (FOIA) request for report DODIG-2015-184, Assessment of the Military Services Insider Threat Programs. We received your request on the same day and assigned it case number FOIA-2016-00016.

The Deputy Inspector General for Intelligence and Special Program Assessments conducted a search and found the enclosed document responsive to your request. I determined that certain redacted portions are exempt from release pursuant to 5 U.S.C. § 552(b)(5), which pertains to certain inter-and-intra agency communications protected by the deliberative process privilege; 5 U.S.C. § 552(b)(6), which pertains to information, the release of which would constitute a clearly unwarranted invasion of personal privacy; and 5 U.S.C. § 552(b)(7)(E), which pertains to records or information compiled for law enforcement purposes, the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions.

Additionally, in coordination with the Department of the Air Force, Department of the Army, Department of the Navy, the Defense Information Systems Agency, and the Office of the Secretary of Defense/Joint Staff, further portions of information are exempt from release in accordance with the following FOIA exemptions:

- Department of the Air Force: 5 U.S.C. § 552 (b)(1), which pertains to information that is currently and properly classified pursuant to Executive Order 13526, section 1.4(a), which pertains to military plans, weapons systems, or operations; and section 1.4(g), which pertains to vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security. Other portions are exempt from release pursuant to 5 U.S.C. § 552(b)(7)(E);
- Department of the Army: 5 U.S.C. § 552(b)(1), section 1.4(c), which pertains to intelligence activities (including covert action), intelligence sources or methods, or cryptology; and section 1.4(g). Additional portions of information are exempt under 5 U.S.C. § 552(b)(3), which pertains to information exempted from release by statute, in this instance 10 U.S.C. § 130, which pertains to unclassified technical data with military or space applications; 5 U.S.C. § 552(b)(5); and 5 U.S.C. § 552(b)(7)(E);

February 23, 2018
Ref: FOIA-2016-00016

- Department of the Navy: 5 U.S.C. § 552(b)(1), section 1.4(g) and; 5 U.S.C. § 552(b)(7)(E);
- Defense Information Systems Agency: 5 U.S.C. § 552(b)(7)(E) and;
- Office of the Secretary of Defense/Joint Staff: 5 U.S.C. § 552(b)(1), section 1.4(c); 5 U.S.C. § 552(b)(3), 10 U.S.C. § 130; 5 U.S.C. § 552(b)(5) and; 5 U.S.C. § 552(b)(6).

If you consider this an adverse determination, you may appeal. You may submit an appeal to the Department of Defense, Office of Inspector General, ATTN: FOIA Appellate Authority, Suite 10B24, 4800 Mark Center Drive, Alexandria, VA 22350-1500. Your appeal, if any, must be postmarked within 90 days of the date of this letter and reference the file number above. I recommend that your appeal and its envelope both bear the notation "Freedom of Information Act Appeal."

You may seek dispute resolution services and assistance with your request from the DoD OIG FOIA Public Liaison Officer at 703-604-9785, or the Office of Government Information Services (OGIS) at 877-684-6448, ogis@nara.gov, or <https://ogis.archives.gov/>. Please note that OGIS mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. However, OGIS does not have the authority to mediate requests made under the Privacy Act of 1974 (request to access one's own records).

If you have any questions regarding this matter, please contact the Department of Defense, Office of Inspector General FOIA Requester Service Center at 703-604-9775 or via email at foiarequests@dodig.mil.

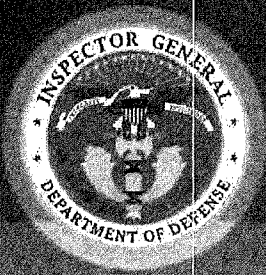
Sincerely,



Mark Dorgan
Division Chief
FOIA, Privacy and Civil Liberties Office

Enclosure(s):
As stated

SECRET//NOFORN



INSPECTOR GENERAL

Department of Defense

September 29, 2015

Report No. DODIG-2015-184

Assessment of the Military Services' Insider Threat Programs (U)

Classified By: DoD OIG: (b) (6) /ISPA
Derived From: (U) U.S. Insider Threat SCG V. 0 16 December 2013
Declassify on: 40 400915

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

SECRET//NOFORN

~~SECRET//NOFORN~~

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.



Fraud, Waste & Abuse

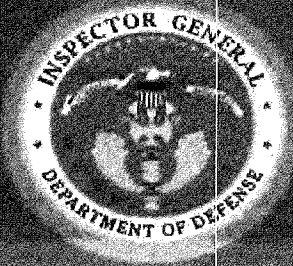
HOTLINE

Department of Defense

dodig.mil/hotline 800.424.8098

For more information about whistleblower protection, please see the inside back cover.

~~SECRET//NOFORN~~



Results in Brief

Assessment of the Military Services' Insider Threat Programs (U)

September 29, 2015

Objective

(U) We conducted this assessment to determine the level of compliance of the Military Services with Executive Order 13587 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs with implementing user activity monitoring.

Finding

(U) The Military Services are not yet fully compliant in meeting the Insider Threat minimum standards because they lacked:

- Implementation guidance from the DoD level insider threat senior official.
- Consistent DoD level insider threat program resources.

Recommendations

We recommend that the Under Secretary of Defense for Intelligence comply with DoDD 5205.16 to facilitate establishing the Military Services' insider threat program by:

Visit us at www.dodig.mil

Recommendations (cont'd)

- (U) Establishing an office of primary responsibility,
- (U) Developing a plan to fully fund the DoD insider threat program, and
- (U) Development of a DoD level Insider Threat implementation plan.

(U) We recommend that the Military Services comply with the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs and DoDD 5205.16 in order to reduce the threat of insider threats.

Management Comments

(U) The Director for Defense Intelligence, on behalf of the Under Secretary of Defense for Intelligence, concurred with all recommendations in the report.

(U) The U.S. Army's Director G-34, on behalf of the Chief of Staff, non-concurred with recommendation 2.e. However, the response provided met the intent of the recommendation requiring no further action. The Director concurred with all other recommendations in the report.

(U) The U.S. Navy's Director of Navy Staff, on behalf of the Chief of Naval Operations; the U.S. Air Force's Administrative Assistant, on behalf of the Chief of Staff; and the U.S. Marine Corps' Assistant Deputy Commandant, on behalf of the Commandant of the Marine Corps, concurred with all recommendations in the report.

000000-2015 (341)

(U) Recommendations Table

| Management | Recommendations Requiring Comment | No Additional Comment Required |
|---|--------------------------------------|-----------------------------------|
| Under Secretary of Defense for Intelligence | | 1.a, 1.b, 1.c |
| Chief of Staff, U.S. Army | | 2.a, 2.d, 2.e |
| Chief of Naval Operations | | 2.a, 2.c, 2.d, 2.e |
| Chief of Staff, U.S. Air Force | | 2.a, 2.c, 2.d, 2.e |
| Commandant of the Marine Corps | | 2.a, 2.b, 2.c, 2.d, 2.e |

(This table is UNCLASSIFIED)



~~SECRET//NOFORN~~

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

September 29, 2015

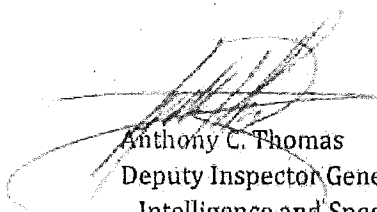
MEMORANDUM FOR UNDERSECRETARY OF DEFENSE FOR INTELLIGENCE
CHIEF OF STAFF, UNITED STATES ARMY
CHIEF OF NAVAL OPERATIONS
CHIEF OF STAFF, UNITED STATES AIR FORCE
COMMANDANT OF THE MARINE CORPS

SUBJECT: Assessment of the Military Services' Insider Threat Programs (U)
(Report No. DODIG-2015-184)

(U) We are providing this report for your information and use. We found that the Military Services were not fully compliant in meeting the minimum standards identified in the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 12, 2012. We conducted this assessment in accordance with the Council of Inspectors General on Integrity and Efficiency Quality Standards for Inspection and Evaluation.

(U) We considered management comments when preparing the final report. The Under Secretary of Defense for Intelligence concurred with all recommendations; the U.S. Army concurred with recommendations 2.a and 2.b, but non-concurred with recommendation 2.e, but their response met the intention of our recommendation requiring no further action; the U.S. Navy concurred with all recommendations, the U.S. Air Force concurred with all recommendations; and the U.S. Marine Corps concurred with all recommendations. Therefore, no additional actions or comments are required.

(U) We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 882-4860 DSN 499-4860.


Anthony C. Thomas
Deputy Inspector General for
Intelligence and Special
Program Assessments

~~SECRET//NOFORN~~

(U) Contents

| | |
|---|----|
| (U) Introduction | I |
| (U) Objective | 1 |
| (U) Background | 1 |
| (U) Finding | 3 |
| (U) Military Services are not yet Fully Compliant with the Insider Threat Minimum Standards | 3 |
| (U) Under Secretary of Defense for Intelligence | 3 |
| (U) Under Secretary of Defense Comptroller | 5 |
| (U) Defense Information Systems Agency | 5 |
| (U) Networks Monitoring Tools | 6 |
| (U) Status of the Military Services' Insider Threat Programs | 7 |
| (U) U.S. Army | 7 |
| (U) Army User Activity Monitoring Program | 8 |
| (U) U.S. Navy | 11 |
| (U) Navy User Activity Monitoring Program | 12 |
| (U) U.S. Air Force | 14 |
| (U) Air Force User Activity Monitoring Program | 15 |
| (U) U.S. Marine Corps | 18 |
| (U) Marine Corps User Activity Monitoring Program | 18 |
| (U) Conclusion | 20 |
| (U) Recommendations, Management Comments, and Our Response | 21 |
| (U) Recommendation 1 | 21 |
| (U) Under Secretary of Defense for Intelligence Comments | 21 |
| (U) Our Response | 22 |
| (U) Recommendation 2 | 22 |
| (U) U.S. Army Comments | 23 |
| (U) Our Response | 24 |
| (U) U.S. Navy Comments | 25 |
| (U) Our Response | 26 |
| (U) U.S. Air Force Comments | 26 |
| (U) Our Response | 27 |
| (U) U.S. Marine Corps Comments | 27 |

| | |
|--|----|
| (U) Our Response..... | 29 |
| (U) Appendix A | 30 |
| (U) Scope and Methodology..... | 30 |
| (U) Use of Computer-Processed Data..... | 31 |
| (U) Prior Coverage..... | 31 |
| (U) GAO..... | 31 |
| (U) Appendix B (Insider Threat Policy) | 32 |
| (U) Policy Development..... | 32 |
| (U) Presidential Policy Initiatives..... | 32 |
| (U) Executive Order 13587..... | 32 |
| (U) National Policy and Minimum Standards..... | 32 |
| (U) Intelligence Community Policy Initiatives..... | 33 |
| (U) IC Standards..... | 33 |
| (U) Committee for National Security Systems..... | 34 |
| (U) Department of Defense Policy Initiatives..... | 36 |
| (U) Undersecretary of Defense for Intelligence..... | 36 |
| (U) Military Service Insider Threat Policies..... | 36 |
| (U) U.S. Army..... | 36 |
| (U) U.S. Navy and U.S. Marine Corps..... | 37 |
| (U) U.S. Air Force..... | 38 |
| (U) Appendix C..... | 39 |
| (U) Organizations Visited and Contacted..... | 39 |
| (U) Management Comments..... | 40 |
| (U) Office of the Under Secretary of Defense, Director for Defense Intelligence (Intelligence & Security)..... | 40 |
| (U) U.S. Army, Deputy Chief of Staff, Director, G-34..... | 42 |
| (U) U.S. Navy, Staff of Chief of Naval Operations..... | 44 |
| (U) U.S. Air Force, Chief of Staff..... | 47 |
| (U) U.S. Marine Corps, Assistant Deputy Commandant, Plans, Policies, and Operations (Security)..... | 49 |
| (U) Acronyms and Abbreviations..... | 54 |

(U) Introduction

(U) Objective

(U) We conducted this assessment to determine the level of compliance that Military Services implemented toward Defense and National Insider Threat (InT) Policies, including initiatives to address threat mitigation and vulnerability reduction.

(U) We focused our assessment on the minimum standards identified in the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 12, 2012 (hereafter referred to as minimum standards). The minimum standards include the capability to gather, integrate, and centrally analyze and respond to key threat-related information; monitor employee use of classified networks; continued evaluation of personnel security information; and provide the workforce with insider threat awareness training. Of all the minimum standards, we only reviewed the status of the user activity monitoring capabilities (UAM) within the Military Services aspect of the minimum standards. The analytical capability and continuous evaluation aspects of the minimum standards were still in development and could not be reviewed at this time.

(U) Background

(U) The concept of insider threats is not new. Recent insider incidents have been highlighted by the crimes committed by former FBI Agent Robert P. Hanssen - 2001; former Defense Intelligence Agency senior analyst, Ana B. Montes - 2001; former U.S. Army Private First Class Bradley E. Manning - 2010 (currently known as Chelsea E. Manning); and leaks of classified information to mainstream media allegedly by former National Security Agency computer professional, Edward J. Snowden - 2013.

(U) After the 2010 classified information disclosures, President Obama issued Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011 (E.O. 13587), which was followed by the minimum standards on November 12, 2012. DoD Directive 5205.16, "The DoD Insider Threat Program" (DoDD 5205.16), September 30, 2014 (See Appendix B), was published during this project. DoDD 5205.16 not only implements the guidance identified in E.O. 13587 and the

minimum standards but also expands the minimum standards to DoD information networks.

(U) E.O. 13587 and the minimum standards mandated the Military Services establish their Insider Threat (InT) Programs on classified networks by conforming to the minimum standards. This initial mandate did not provide dedicated insider threat funding causing the Military Services to execute their programs from existing internal budgets¹. As a result, the Military Services slowly moved forward with the development of their InT programs and UAM implementation.

(U//~~FOUO~~) E.O. 13587 created the National Insider Threat Task Force to create national level insider threat policy and help Executive Branch Agencies with the implementation of their insider threat programs. To do this, the NITTF published a "Guide to accompany the National Insider Threat Policy and Minimum Standards" in November 2013. This guide states Agencies "should establish a program office" to execute InT policy and program implementation plan.

(U//~~FOUO~~) Some financial assistance was offered by the Office of the Director of National Intelligence (ODNI) to the Intelligence Community, which include the military intelligence components of the Military Services, in the development of UAM capabilities on the Joint Worldwide Intelligence Community System (JWICS).

(U) We will provide a copy of the final report to the USD(I) and senior officials responsible for internal controls in the Army, Navy, Air Force, and Marine Corps.

¹ (U) Budgets were reduced because of the Budget Sequestration taking effect in 2013 which refers to automatic spending cuts of about \$1 trillion to the U.S. Federal Government, and the proposed FY 2015 Defense Budget which is \$0.4 billion less than enacted in FY 2014 appropriation.

(U) Finding

(U) Military Services are not yet Fully Compliant with the Insider Threat Minimum Standards

(U) The Military Services' InT programs lack:

- (U) Implementation guidance from the DoD level insider threat senior official, and
- (U) Consistent DoD level Insider Threat program resources.

(U//~~FOUO~~) Because the DoD level InT policy was not issued in a timely manner, most of the Military Services generated their own InT programs based on the requirements identified in E.O. 13587 and the minimum standards. Although DoDD 5205.16 has been issued, the Military Services are still waiting for implementing guidance from USD(I). Additionally, the Under Secretary of Defense - Comptroller does not have any specific insider threat funds. Lastly, the Defense Information Support Agency does provide some network monitoring tools and monitoring services to the Military Services, but the tools do not meet the specific need of user activity monitoring as outlined in the minimum standards.

(U) Under Secretary of Defense for Intelligence

(U//~~FOUO~~) In a February 2011 memorandum, the Secretary of Defense directed the Assistant Secretary of Defense for Homeland Security and Americas' Security Affairs (ASD[HD&ASA]) to establish a DoD Insider Threat program. In September 2013, the Secretary of Defense designated the USD(I) as the insider threat senior official. Upon assuming the duties as the insider threat senior official, the USD(I) took over drafting


1010-200-101

~~SECRET//NOFORN~~

the insider threat directive that ASD(HD&ASA) started in 2011. DoDD 5205.16, published on September 30, 2014, establishes policy and assigns responsibilities within DoD for developing and maintaining an InT program. The InT program must comply with the requirements and minimum standards to prevent, deter, and mitigate actions by malicious insiders who represent a threat to national security or DoD personnel, facilities, operations, and resources. Additionally, the USD(I) is responsible to establish an implementation plan, which is currently in coordination for comments.

(S//NF)

ARMY: (b) (1), EO 13526, secs. 1.4(c), 1.4(g); OSD/JS: (b) (1), EO 13526, sec. 1.4(c)



(U//FOUO) In accordance with DoDD 5205.16, USD(I) is responsible for providing management, accountability, and oversight of the DoD InT program. We determined that USD(I) provides minimal oversight to the InT program based on the following information:

- (U//FOUO) The USD(I) Deputy Director for Security and Insider Threat, OSD/JS: (b) (6), stated that USD(I) did not receive any feedback from the Military Services after the release of DoDD 5205.16, prompting him to ask us during the interview how the Military Services' InT programs are doing.
- (U//FOUO) OSD/JS: (b) (6) also informed us that the lack of a singular InT office was an issue and that there should be a central point that DoD officials could reach out to for information or questions related to InT.

~~SECRET//NOFORN~~

(U) Under Secretary of Defense Comptroller


(U//~~FOUO~~) An OUSD(C) SME stated that InT is an evolving concept and that there is no one definition for insider threat yet. No centralized budgets for InT have been established, but there are cyber monitoring line items within the Chief Information Officer's (CIO) budget. A large portion of the cyber budget items is found in the consolidated cryptographic program (CCP), which is part of the NIP portfolio. The OUSD(C) SME stated he does not expect InT funding this budget cycle. He also said there should be more funding within future annual budgets, but the funding will likely arrive after a cyber justification is agreed upon.

(U//~~FOUO~~) ARMY: (b) (5), (b) (7)(E)

A large rectangular area of the document is redacted with black ink, covering approximately four lines of text.

(U) Defense Information Systems Agency

(U//~~FOUO~~) DISA: (b) (7)(E)

A large rectangular area of the document is redacted with black ink, covering approximately ten lines of text.

(U//~~FOUO~~) [REDACTED] DISA: (b) (7)(E)
[REDACTED] DISA: (b) (7)(E); OSD/JS: (b) (3), 10 USC § 130 DISA: (b) (7)(E)
[REDACTED]
[REDACTED] DISA: (b) (7)(E), OSD/JS: (b) (3), 10 USC § 130
DISA: (b) (7)(E)
[REDACTED]
[REDACTED] DISA: (b) (7)(E); OSD/JS: (b) (3), 10 USC § 130 DISA: (b) (7)(E)
[REDACTED]

(U//~~FOUO~~) [REDACTED] DISA: (b) (7)(E) [REDACTED] DISA: (b) (7)(E); OSD/JS: (b) (3), 10 USC § 130 [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] DISA: (b) (7)(E); OSD/JS: (b) (3), 10 USC § 130 DISA: (b) (7)(E)
[REDACTED]
[REDACTED]

(U//~~FOUO~~) [REDACTED] DISA: (b) (7)(E)
[REDACTED] DISA: (b) (7)(E); OSD/JS: (b) (3), 10 USC § 130
[REDACTED]
[REDACTED]

(U) Networks Monitoring Tools

(U//~~FOUO~~) We determined the current tool that the Services are using for UAM is

OSD/JS: (b) (3), 10 USC § 130, ARMY: (b) (3), 10 USC § 130, (b) (7) [REDACTED] ARMY: (b) (3), 10 USC § 130, (b) (7)(E)
[REDACTED]
[REDACTED] OSD/JS: (b) (3), 10 USC § 130 ARMY: (b) (3), 10 USC § 130, (b) (7)(E)
[REDACTED] OSD/JS: (b) (3), 10 USC § 130 ARMY: (b) (3), 10 USC § 130, (b) (7)(E)
[REDACTED]

(U//~~FOUO~~) [REDACTED] ARMY: (b) (5), (b) (7)(E)
[REDACTED] The Marine

Corps' UAM program is the newest, having been ready for operations since September 2014, but has not received approval to operate on the USMC JWICS network as of March 2015. ARMY: (b) (3), 10 USC § 130, (b) (7)(E)

(U) Status of the Military Services' Insider Threat Programs

(U) We reviewed the status and capabilities of the Military Services' InT programs. We limited our scope to the ARMY: (b) (7)(E)

(U) U.S. Army

(S//NF) OSD/JS: (b) (1), EO 13526, sec. 1.4(c); ARMY: (b) (1), EO 13526, sec. 1.4(c)

(U//FOUO) ARMY: (b) (5), (b) (7)(E)

² (U) Principle Guiding Documents are E.O. 13587 and the, National Insider Threat Policy and Minimum Standards. See Appendix B.

000000

ARMY: (b) (5), (b) (7)(E)

[REDACTED]

(U//~~FOUO~~) ARMY: (b) (5), (b) (7)(E)

[REDACTED]

• (U//~~FOUO~~) ARMY: (b) (5), (b) (7)(E)

[REDACTED]

• (U//~~FOUO~~) ARMY: (b) (5), (b) (7)(E)

[REDACTED]

• (U//~~FOUO~~) ARMY: (b) (5), (b) (7)(E)

[REDACTED]

(U) Army User Activity Monitoring Program

(U//~~FOUO~~) ARMY: (b) (3), 10 USC § 130, (b) (5), (b) (7)(E)

[REDACTED]

OSD/JS: (b) (3), ARMY: (b) (3), 10 USC § 130, (b) (5), (b) (7)(E)
10 USC § 130

OSD/JS: (b) (3), 10 USC § 130,
ARMY: (b) (3), 10 USC § 130, (b)

(U//~~FOUO~~) The Army has approximately [REDACTED] workstations. [REDACTED] ARMY: (b) (5), (b) (7) (E)

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] The privileged users are the computer operators who are in positions of greater network privileges, such as system administrators. [REDACTED] ARMY: (b) (5), (b) (7) (E)

[REDACTED]
[REDACTED]

(U//~~FOUO~~) The Army acquired HBSS from DISA in 2010, because the software was free; however, the hardware was not free. HBSS was marketed to the Army as an antivirus program with a device control module. The Army also activated a rouge system detector module.

(U//~~FOUO~~) The Army conducted a pilot program with the [REDACTED] OSD/JS: (b) (3), 10 USC § 130
tools from 2011 to 2012 at the National Ground Intelligence Center (NGIC). [REDACTED] ARMY: (b) (3), 10 USC § 130, (b) (5), (b) (7) (E)

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] OSD/JS: (b) (3), ARMY: (b) (3), 10 USC § 130, 10 USC § 130
[REDACTED] (b) (5), (b) (7) (E)
[REDACTED] OSD/JS: (b) (3), 10 USC § 130; ARMY: (b) (3), 10 USC § 130, (b) (5), (b) (7) (E)
[REDACTED]

000000

(U//~~FOUO~~) When an attributable and auditable event (trigger), trips in
OSD/JS (b) (3), 10 /HBSS OSD/JS (b) (3), an AJNAP Analyst reviews the data and writes an incident
USC § 130 (b) (3), 10 USC § 130 assessment report (IAR). IARs are balanced against an organization's mission and what
is currently going on in the world. ARMY: (b) (5), (b) (7)(E)

[REDACTED]

(U//~~FOUO~~) The Army gets its triggers from ICS 500-27, "Collection and Sharing of
Audit Data," June 2, 2011. ARMY: (b) (5), (b) (7)(E)

[REDACTED]

(U//~~FOUO~~) ARMY: (b) (3), 10 USC § 130, (b) (5), (b) (7)(E)

[REDACTED]

(U//~~FOUO~~) According to an Army SME, ARMY: (b) (5), (b) (7)(E)

[REDACTED]

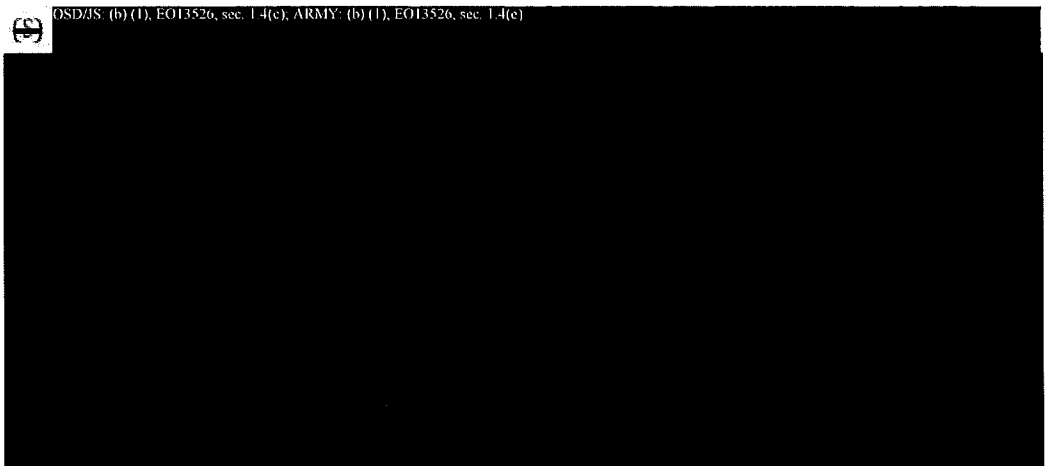
(U) ARMY: (b) (5), (b) (7)(E)

[REDACTED]

000000

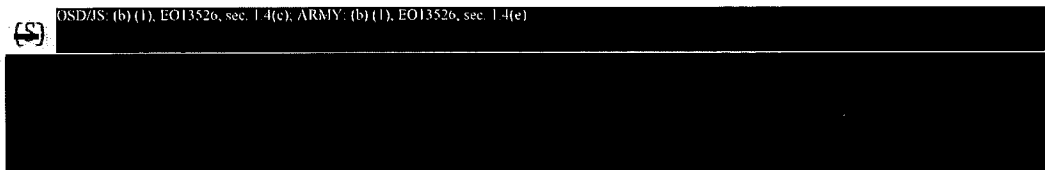
(S)

OSD/JS: (b) (1), EO13526, sec. 1.4(c); ARMY: (b) (1), EO13526, sec. 1.4(c)



(S)

OSD/JS: (b) (1), EO13526, sec. 1.4(c); ARMY: (b) (1), EO13526, sec. 1.4(c)



(U) U.S. Navy

(U//~~FOUO~~) The Department of the Navy (DON), unlike the other Military Departments, is responsible for two Military Services, the Navy and the Marine Corps. Instead of waiting on the completion of the DoD Directive, the DON published Secretary of the Navy Instruction (SECNAVINST) 5510.37, "Department of the Navy Insider Threat Program," August 8, 2013 (see Appendix B) charging the Navy and the Marine Corps to establish their InT programs. Additionally, it identifies the Deputy Under Secretary of the Navy for Plans, Policy, Oversight and Integration (PPOI) as the senior executive responsible for the DON InT management.

(U//~~FOUO~~) The Navy initiated its InT program based on E.O. 13587 and the minimum standards, but has been unable to meet compliancy with the minimum standards due to UAM not being implemented on each of the classified networks. We determined that a lack of Department level guidance and InT resources was the primary reasons for the

(U//~~FOUO~~)

shortfalls. The Director of the Navy Staff leads the Navy's InT program. The Navy published Chief of Naval Operations Instruction (OPNAVINST) 5510.165, "Navy Insider Threat Program," on January 27, 2015 (see Appendix B).

(U//~~FOUO~~) The Navy's InT SME stated that the Navy received InT program guidance without additional funding³ allotted for its implementation. As Navy money was already allocated, Navy had to realign funding to support its InT program. The Navy's InT program personnel are engaged with the National Insider Threat Task Force (NITTF) for funding⁴ to cover program resource shortfalls and to ensure that Navy has funding for the program through FY 2015.

(U//~~FOUO~~) The N2N6 (Information and Cyber) is currently working on the Navy's InT implementation plan. The Navy contracted with the Navy's Space and Naval Warfare Systems Command (SPAWAR), in conjunction with Carnegie Mellon University, to review resource requirements the Navy needs to build an effective InT program. This study concluded in May 2015, and its details were presented at the Navy Executive Brief in June 2015. Findings from the study will impact the Navy's Insider Threat Implementation Plan because they include recommendations for information technology architecture, broad resource requirements, and high level strategy to establish and sustain enterprise-wide UAM and Analysis Hubs.

(U) Navy User Activity Monitoring Program

(U) The Navy is focusing its UAM resources to cover all Navy JWICS in FY 2015 and FY 2016 based on risk management decisions. The Navy plans to initiate UAM efforts on SIPRNET following coverage of all Navy JWICS.

(U//~~FOUO~~) The Navy implemented the JWICS UAM program within the Office of Naval Intelligence (ONI), when they had a UAM pilot program in 2012. ONI receives guidance

³ (U) Evaluator Comment: Additional funding pertains to InT program funding allocated in the National Defense Authorization Act.


⁴ (U) While the NITTF does not provide funding, the DON appears to be using the NITTF to advocate funding for them.

~~SECRET//NOFORN~~

and funding from the ODNI as well as the Navy. ONI leadership's guidance was to approach the program implementation with a crawl, walk, run concept to ensure ONI implements a solid program.

(S//NF)

OSD/JS: (b) (1), EO13526, sec. 1.4(c); NAVY: (b) (1), EO13526, sec. 1.4(g)




(U//FOUO)

NAVY: (b) (1), EO13526, sec. 1.7(e)




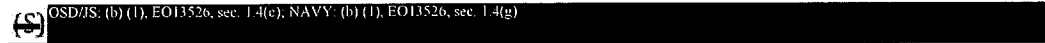
(S)

OSD/JS: (b) (1), EO13526, sec. 1.4(c); NAVY: (b) (1), EO13526, sec. 1.4(g)



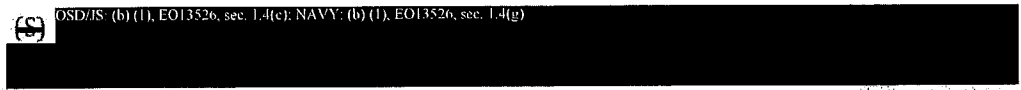
(S)

OSD/JS: (b) (1), EO13526, sec. 1.4(c); NAVY: (b) (1), EO13526, sec. 1.4(g)



(S)

OSD/JS: (b) (1), EO13526, sec. 1.4(c); NAVY: (b) (1), EO13526, sec. 1.4(g)




~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

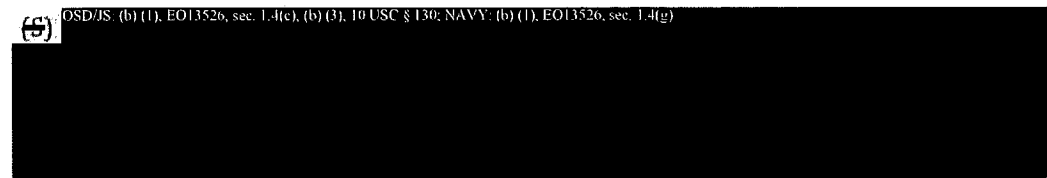
OSD/JS: (b) (1), EO13526, sec. 1.4(c), (b) (3), 10 USC § 130; NAVY: (b) (1), EO13526, sec. 1.4(g)



(S) OSD/JS: (b) (1), EO13526, sec. 1.4(c), (b) (3), 10 USC § 130; NAVY: (b) (1), EO13526, sec. 1.4(g)




(S) OSD/JS: (b) (1), EO13526, sec. 1.4(c), (b) (3), 10 USC § 130; NAVY: (b) (1), EO13526, sec. 1.4(g)



(U) U.S. Air Force

(S//NF) OSD/JS: (b) (1), EO13526, sec. 1.4(c), (b) (3), 10 USC § 130; USAF: (b) (1), EO13526, sec. 1.4(a), 1.4(g)



(U//~~FOUO~~) Air Force Instruction 16-1402, "Insider Threat Program Management," was published on August 5, 2014. The Air Force InT program is led by the Administrative Assistant of the Secretary of the Air Force, with the Policy and Security Enterprise Division (SAF/AAZE) as the main action office. The Air Force contracted with Carnegie Mellon University to review resource requirements the Air Force needs to build an effective insider threat program. The Air Force implementation plan is in the coordination process. The Air Force UAM is conducted from Air Force Intelligence,

~~SECRET//NOFORN~~

Surveillance, and Reconnaissance Agency (AFISRA), which also hosts the Air Force's Intelligence Community Security Coordination Center (IC SCC) – where the centralized analysis and response capability is established. The 24th Air Force (Cyber) sends its cyber audit and data to AFISRA for analysis.

(U//~~FOUO~~) AFISRA started working on the InT program in January 2014, and deployed it in April 2014. The AFISRA UAM program is prioritizing privileged users to be subject to UAM. USAF (b) (5), (b) (7)(E)

Another AFISRA SME stated that UAM is a priority for JWICS, and then it will be rolled out to weapons systems, such as Distributed Common Ground System (DCGS) and ISR platforms because these systems are additional networks on AF JWICS.

(U) Air Force User Activity Monitoring Program

(U) The Air Force does not have specific policies for cyber InT monitoring in regard to insider threat for SIPRNET. However, there are a variety of defensive/preventive measures in place to combat the insider threat. These measures include periodic review of privileged users need for privileged capabilities or access, periodic revalidation of domain administrator accounts to prove need for rights, two-person integrity for privileged administrators, user and administrator logging, limiting the rights the administrators have to core areas, and limiting the number of administrators with full rights to a select few across the enterprise. While audit logs are collected, there is no specific UAM program for SIPRNET.

(U//~~FOUO~~) Current SIPRNET network monitoring is conducted by the 24th Air Force. The monitoring mission is split between the 33rd Network Operations Squadron in San Antonio, the 83rd Network Operations Squadron at Langley AFB, VA, and the 561st Network Operations Squadron at Peterson AFB, CO. The three squadrons receive network alerts via the HBSS, which is a DoD standard. We determined that the Air Force is challenged in content monitoring of the network traffic due to the programs that they are using. The AF is responsible for monitoring at the

~~SECRET//NOFORN~~

000000

workstation/base/Service level, which it does concurrently on the NIPRNET and SIPRNET.

(U//~~FOUO~~) The Air Force has ~~USAF: (b) (7)(E)~~. AF JWICS have a UAM program working already. This UAM program works in conjunction with ~~OSD/JS: (b) (3), 10 USC 8~~ event manager, which collects and archives system event audit logs for information assurance activities.

(U//~~FOUO~~) ~~USAF: (b) (7)(E)~~
~~[REDACTED]~~
~~[REDACTED]~~
~~[REDACTED]~~
~~[REDACTED]~~
~~[REDACTED]~~

(S//NF) ~~OSD/JS: (b) (1), EO 13526, sec. 1.4(c); USAF: (b) (1), EO 13526, secs. 1.4(a), 1.4(g)~~
~~[REDACTED]~~

(U//~~FOUO~~) AFISRA started working on the InT program in January 2014 and deployed it in April 2014. The AFISRA UAM program is prioritizing privileged users to be subject to UAM monitoring. ~~USAF: (b) (5), (b) (7)(E)~~
~~[REDACTED]~~

Another AFISRA SME stated that UAM is a priority for JWICS, then it will be rolled out to weapons systems, such as Distributed Common Ground System (DCGS) and ISR platforms because these systems are additional networks on AF JWICS.

(U//~~FOUO~~) Integration of the AF InT program is in three phases:

- (U//~~FOUO~~) Phase one is deployment of UAM to AF JWICS;

~~SECRET//NOFORN~~

- (U//~~FOUO~~) Phase two is deployment of UAM to weapon systems, such as DCGS; and
- (U//~~FOUO~~) Phase three is deployment of UAM to SIPRNET and NIPRNET. Planning, design, programming, development, deployment and execution of each phase will occur in a nonlinear fashion and as dictated by budgetary reality.

(S//NF) [REDACTED] USAF (b) (1), EO13526, secs. 1.4(a), 1.4(g)

[REDACTED] OSD/JS (b) (3), USAF (b) (1), EO13526, secs. 1.4(a), 1.4(g)

(U//~~FOUO~~) The Air Force operates five SAP networks within its enterprise. When an anomaly is discovered in the network activity, it is viewed only within the confines of that particular network. The Network Operations Centers occasionally communicate with each other when there is common vulnerability or details of an anomaly that can be shared without violating the SAP's integrity.

(U//~~FOUO~~) The Air Force intends to have the SAP networks monitored at the same level as JWICS. The main difference is that the SAP network monitoring will not be an enterprise effort but a general capability covering the SAP platforms. Currently, there are not any UAM tools on the SAP networks, but the Air Force is testing some for deployment.

(U//~~FOUO~~) The Air Force is not fully compliant with the minimum standard of implementation of UAM on its JWICS system. The Air Force is not compliant with UAM implementation on its SIPRNET and SAP networks.

(U) U.S. Marine Corps

(U//~~FOUO~~) The Marine Corps started an InT program is led by a working group which consists of representatives from USMC CIO, Counterintelligence/Human Intelligence, civilian and military representatives from human capital, resource management, General Counsel, and the InT Program Manager. The Marine Corps' InT program resides in Plans, Policy, and Operations (PP&O). The Marine Corps' InT representative participates in the DON InT working group.

(S//~~INTEL~~) OSD/JS: (b) (1), EO13526, sec. 1.4(c)

(U//~~FOUO~~) While the Marine Corps is focused on [DoD OIG: (b)(5), (b)(7)(E)]

(U) Marine Corps User Activity Monitoring Program

(U//~~FOUO~~) The Marine Force Cyber Command is currently using [DoD OIG: (b)(5), (b)(7)(E)]

DoD OIG (b)(5), (b)(7)(E)

(U//~~FOUO~~) The Marine Corps Intelligence Activity (MCIA) developed its insider threat program pursuant to IC requirements, specifically ICS 700-2, "Use of audit data for insider threat," and IC funding. The developed model will be implemented to the USMC Expeditionary Force level through the Marine Corps Intelligence, Surveillance, Reconnaissance Enterprise (MCISRE) and USMC JWICS Enterprise during FY 2015 and FY 2016.

(S//~~NF~~) OSD/JS (b) (1), EO 13526, sec. 1.4(c)

(U//~~FOUO~~) DoD OIG (b)(5), (b)(7)(E)

In 2015, the JWICS UAM will extend to the rest of the USMC, including the Marine Corps University, I Marine Expeditionary Force, along with the other Marine Expeditionary Forces, and finally the rest of the Marine Corps JWICS enterprise.

(U//~~FOUO~~) The USMC JWICS UAM program is on a separate JWICS enclave with only a few personnel with access to it. A two-person integrity rule for system and hardware changes or updates is required. This includes both ISD and InT program persons.

(U//~~FOUO~~) The UAM triggers provide data and video capture to the Information Assurance Manager (IAM) to review. If the event requires further review, then the IAM

will pass the data to the InT program Manager to check other data bases. The InT PM will send the incident report to the InT working group to get approval to do an inquiry and analysis. This could result in a report to the commanding officer of the suspect or an incident report to NCIS.

(U//~~FOUO~~) The USMC InT program is working on a cross domain solution in FY 2015. They are licensing an open source information system, which could bring information up to JWICS for analysis.

(U//~~FOUO~~) DoD OIG: (b)(5), (b)(7)(E)

(U) Conclusion

(U//~~FOUO~~) ARMY: (b)(5), (b)(7)(E)

Insider threat is recognized within all branches of the United States Government as a viable threat capable of causing grave damage to national security. In the absence of DoD policy, the Military Services created InT programs based on the principal guidance within E.O. 13587 and the minimum standards. DoDD 5205.16 codified existing guidance into DoD policy regarding the DoD InT implementation plan, which is still in the coordination phase.

(U//~~FOUO~~) The InT program is vital to national security and should have its own budget funding line. ARMY, USAF: (b)(5), (b)(7)(E)

A possible solution, which has already been identified in the NITTF, "Guide to Accompany the National Insider Threat Policy and Minimum

Standards," and the DoDD 5205.16, is to establish the InT program office within the USD(I). Additionally, the Military Services should implement Service level InT program offices applying the same standards as that in the USD(I).

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend the USD(I), as the DoD Insider Threat senior official, establish an Insider Threat Program Office within the USD(I) to fulfill the responsibilities stated in DoDD 5205.16, which include but are not limited to:

- a. (U) Provide for management, accountability, and oversight of the DoD Insider Threat Program,
- b. (U) Make resource recommendations to the Secretary of Defense by developing a plan to fully fund the DoD insider threat program, and
- c. (U) Develop a DoD level insider threat implementation plan.

(U) Under Secretary of Defense for Intelligence Comments

(U) The Director for Defense Intelligence, on behalf of the Under Secretary of Defense for Intelligence concurred with recommendation 1.a., 1.b., and 1.c., providing the following comments:

(U) Recommendation 1.a: "Agree. An internal assessment is being conducted to determine the best organizational structure for the DoD insider threat program office, with feedback expected in December 2015. In the interim, OUSD(I) dedicated staff within the Office of the Director for Defense Intelligence (Intelligence and Security) manage the DoD insider threat program at the enterprise level, and placed a DoD liaison officer at the National Insider Threat Task Force. With the addition of two full-time contractors planned for FY-16,

the DoD Insider Threat Branch will be better positioned to accomplish the management and oversight functions specified in national and DoD insider threat policies."

(U) Recommendation 1.b: "Agree. The Principal Staff Assistant for security and insider threat, the USD(I) has included resource recommendations in the current and previous two Program Budget Review cycles. OUSD(I) is also designing the content and scope of the annual status report to the Secretary of Defense and resource recommendations will be a key component of that report.

OSD/IS: (b) (5)

Additionally, OUSD(I) personnel are reviewing all funding streams that have an insider threat nexus for possible enhancements. OUSD(I) and DoD Components will continue to collaborate on identifying the resources needed, potential sources, and pursuing those actions required to procure them."

(U) Recommendation 1.c: "Agree. The DoD implementation plan has been written and coordinated with all DoD Components. Publication of this plan is projected in the first quarter of CY 16."

(U) The comments of USD(I) for recommendations 1.a., 1.b., and 1.c. were responsive and require no further action.

(U) Recommendation 2

(U) We recommend the U.S. Army – Army Protection Program G-3/5/7, U.S. Navy Plans, Policy, Oversight and Integration (PPOI), U.S. Air Force Policy and Security Enterprise Division (SAF/AAZE), and U.S. Marine Corps Plans, Policies & Operations (PP&O) establish Insider Threat Office of Primary Responsibility to execute the responsibilities

stated in the minimum standards and in DoDD 5205.16, which include but are not limited to:

- a. (U) Implement the user activity monitoring aspect of the Minimum Standards for Executive Branch Insider Threat Programs on all classified networks,
- b. (U) Establish an Insider Threat Program policy,
- c. (U) Establish an InT implementation plan,
- d. (U) Monitor and report progress on the implementation of their insider threat programs, and
- e. (U) Identify internal InT funding requirements in a program objective memorandum to USD(I).

(U//FOUO) Army Comments

(U) The Director, G-34, on behalf of the Chief of Staff, concurred with recommendations 2.a, and 2.d., providing the following comments:

(U//FOUO)

ARMY: (b) (5), (b) (7)(E)


(U)

ARMY: (b) (5), (b) (7)(E)

~~SECRET//NOFORN~~

040411Z

ARMY: (b) (5), (b) (7)(E)



(U) The U.S. Army non-concurred with recommendation 2.e., providing the following comments:

(U)

ARMY: (b) (5), (b) (7)(E)



(U) Our Response

(U) The comments of the U.S. Army for recommendations 2.a., 2.d., and 2.e. were responsive and require no further action. Although the Army non-concurred with recommendation 2.e., their action to obtain InT funds meets the intent of our recommendation.

040411Z

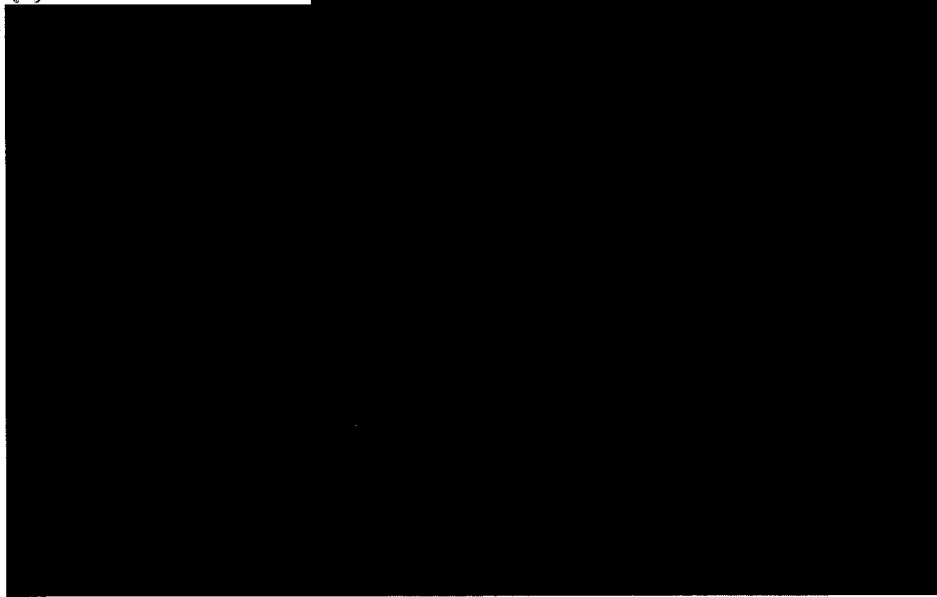
~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) The Director, Navy Staff, on behalf of the Chief of Naval Operations, concurred with recommendations 2.a., 2.c., 2.d., and 2.e., providing the following comments:

(S) Recommendation 2.a:

OSD/JS: (b) (1), EO13526, sec. 1.4(c); NAVY: (b) (1), EO13526, sec. 1.4(g)



(U) Recommendation 2.c: "OPNAV concurs with this recommendation. In June 2015, the DNS drafted an InT Implementation Plan that is in formal policy coordination for review and comment."

(U//~~FOUO~~) Recommendation 2.d: "OPNAV concurs with this recommendation. In October 2015, the DNS will oversee the preparation of an annual report for delivery to the CNO, which provides an update on the completion of requirements found in the InT Implementation Plan, additional accomplishments, resources allocated, insider threat risks identified, recommendations, goals for Program improvement, and that identifies major impediments or challenges. Further, DNS will provide programming recommendations to CNO for Navy Insider Threat. The DNS will facilitate

reviews of the Navy's InT program to ensure compliance with policy guidance, including a requirement to conduct and report self-assessments."

(U//~~FOUO~~) Recommendation 2.e: "OPNAV concurs with recommendation. DNS established the Navy Insider Threat Board of Governance (NITBOG) to provide senior leadership recommended actions, prioritization, planning, programming, information sharing and execution of activities in support of a comprehensive Navy InTP. In July 2015, SPAWAR provided the NITBOG a Navy InT to Cyber Security analysis, which defined and documented existing gaps in InT to Cyber Security controls, and recommend new or modified controls and associated architecture revisions, along with broad resource and manpower requirements, to ensure U.S. navy meets insider threat program requirements."

(U//~~FOUO~~) Recommendation

(U) The comments of the U.S. Navy for recommendations 2.a., 2.c., 2.d., and 2.e. were responsive and require no further action.

(U//~~FOUO~~) Recommendation

(U) The Administrative Assistant, on behalf of the Chief of Staff, concurred with recommendations 2.a., 2.c., 2.d., and 2.e., providing the following comments:

(U//~~FOUO~~) Recommendation 2.a: "The Air Force agrees with this recommendation. The Air Force completed a requirement gap analysis for implementing UAM on all classified networks which identified funding requirements to expand UAM to Special Access Program and SIPR. This requirement is competing for funding in FY15, pending the outcome of reprogramming actions currently in Congress. The Air Force has implemented UAM on portions of the classified network fabric and expects to fully meet the classified network requirement in FY16. The Air Force Security Enterprise Executive Board (AFSEEB) will review status in September and we will fund UAM to the appropriate amounts in accordance with requirements, threat

assessments, and competing priorities. We will use the FY17 PBR and the FY18 POM to implement any funding adjustments."

(U) Recommendation 2.c: "The Air Force agrees with this recommendation. The Air Force completed final functional coordination of its InT Implementation Plan on 9 August 2015 and expects final publication by 4 September 2015."

(U) Recommendation 2.d: "The Air Force agrees with this recommendation. The Air Force reported initial task completion to National Insider Threat Task Force (NITTF) on 26 June 2014 and is scheduled for an assessment by the NITTF on 2 December 2015. The AFSEEB, which includes senior level participation from the intelligence, security forces, acquisition, inspector general, communications, operations, personnel, and nuclear enterprise communities, meet monthly to review InT implementation and work evolving issues."

(U) Recommendation 2.e: "The Air Force agrees with this recommendation. The Air Force completed a cross functional requirement gap analysis on 11 August 2015. The Air Force will address funding in the FY18 POM.

Joint Air Response

(U) The comments of the U.S. Air Force for recommendations 2.a., 2.c., 2.d., and 2.e. were responsive and require no further action.

U.S. Marine Corps Comments

(U) The Assistant Deputy Commandant for Plans, Policies, and Operations, on behalf of the Commandant of the Marine Corps, concurred with recommendations 2.a., 2.b., 2.c., 2.d., and 2.e., providing the following comments:

(U) Recommendation 2.a: "CONCUR. Current UAM (and audit) is being conducted at the Marine Corps Intelligence Activity (MCIA) for the Joint Worldwide Intelligence Communications System (JWICS) and there are

discussions underway to expand this capability to the SIPR network via the Cross Domain Solution (CDS). Additionally:

(U) Marine Corps Systems Command (MCSC) is deploying a Host Based Security System (HBSS) Data Loss Prevention (DLP) capability on the SIPR network and user's computers and work solutions.

(U) Three DLP pilots have been completed by Marine Corps Command, Control, Communications, and Computers (C4) and MCSC.

(U) MARFORCYBER is creating an Urgent Needs Statement (UNS) to procure a significant amount of storage capability to better support data and user auditing requirements."

(U) Recommendation 2.b: "CONCUR. Current policy for the Marine Corps Insider Threat Program was promulgated on 10 April, 2015 via MAADMIN 187/15 with the focus on intervention and the prevention of threats which may result in damage or destruction to Marine Corps persons, places, and things. A supporting Marine Corps Order (MCO) is currently being drafted which will include the recent revisions to the Department of Defense (DoD) Insider Threat policy. The estimated signature date for the MCO is 3rd Quarter FY16."

(U) Recommendation 2.c: "CONCUR. Concurrently with the drafting of the supporting MCO, an implementation plan is currently being drafted. The estimated signature date for the implementation plan is 3rd Quarter FY16."

(U) Recommendation 2.d: "CONCUR. Security Branch is currently providing oversight, to include reporting and monitoring, for the development and expansion of the Marine Corps Insider Threat Program."

(U) Recommendation 2.e: "CONCUR. Current Insider Threat requirements are being entered into the Marine Corps Capability Based Assessment (MC-CBA) process. This process includes capabilities, gap, solutions, and risk analysis.

~~SECRET//NOFORN~~

The information derived from this process will inform the investment strategies for the next POM cycle. The estimated completion date for the Capabilities Investment Plan (CIP) submission is 4th Quarter FY16."

(U) This Response

(U) The comments of the U.S. Marine Corps for recommendations 2.a., 2.b., 2.c., 2.d., and 2.e. were responsive and require no further action.

~~SECRET//NOFORN~~

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this assessment from April 2014 through July 2015 in accordance with Council of the Inspectors General on Integrity and Efficiency (CIGIE) Quality Standards for Inspection and Evaluation. Those standards require that we plan and perform the assessment to obtain sufficient, appropriate evidence to provide a reasonable basis for our finding and conclusions based on our audit [or attestation] objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our assessment objectives.

(U//~~FOUO~~) The project scope was limited to the Military Services. We assessed status of the Military Services' Insider Threat Programs and UAM programs to provide an initial baseline of their initial operational capability. Specifically, we focused on the authorities, roles, responsibilities, and available resources. To that end, we visited the different Military Services to determine if there was a level of consistency in the way the DoD Insider Threat Program was organized, delivered, and overseen.

(U//~~FOUO~~) We did not intend to provide an impact assessment of the type of methods used within the Military Services' Insider Threat Programs by showing a success rate. Nor did we audit the financial accounting of the Insider Threat Program.

(U//~~FOUO~~) We reviewed oversight issuances to include laws, Executive Orders, DoD issuances, and Military Services' internal issuances. This information provided the baseline standards for the program and its oversight.

(U) We conducted structured interviews and follow-up discussions by phone and e-mail with the Military Services' points of contact. This information identified the effectiveness of the InT program and how it is managed as well as InT resource allocations at the OUSD(I) and Military Service levels. We also identified the status of the Military Service cyber monitoring efforts.

2016 06 06 08:27

(U) Use of Computer-Processed Data

(U) We did not use computer-processed data to perform this assessment.

(U) Prior Coverage

(U) During the last 5 years, the Government Accountability Office (GAO) conducted one project discussing [DoD's Insider Threat Program]. Unrestricted GAO reports can be accessed at <http://www.gao.gov>.

(U) GAO

(U) GAO-15-357C "Insider Threat: DoD Should Strengthen Management and Guidance to Protect Classified Information and Systems," April 14, 2015.

(U) Appendix B (Insider Threat Policy)

(U) Policy Development

(U) We highlighted relevant policies from national-level down to Service implementation task orders to show the progress being made in policy development. We focused on the policies related to network monitoring and UAM.

(U) Presidential Policy Initiatives

(U) Executive Order 13587

(U) Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," October 7, 2011, brought numerous improvements in classified information sharing and safeguarding. It also established the Insider Threat Task Force (ITTF), co-chaired by the Department of Justice (DOJ) and National Counterintelligence Executive (NCIX). Many executive branch departments and agencies provide representatives to the ITTF. The mission of the task force is to develop a government-wide insider threat program for deterring, detecting, and mitigating insider threats. This activity will cover policies, objectives, and priorities to establish and integrate security, counterintelligence (CI), user audits and monitoring, and other safeguarding capabilities and practices within the agencies.

(U) National Policy and Minimum Standards

(U) The President's National Insider Threat Policy and minimum standards for executive branch insider threat programs was published on November 21, 2012. The ITTF developed and issued the minimum standards and guidance for implementing InT program capabilities, to include monitoring of user activity on United States Government networks. This refers to audit data collection strategies for insider threat detection, leveraging hardware and software with triggers deployed on classified

networks to detect, monitor, and analyze anomalous user behavior for indicators of misuse.

(U) These minimum standards include monitoring user activity on U.S. Government networks; continued evaluation of personnel security information; employee training of insider threat; and analysis, reporting and response. Agency heads will ensure insider threat programs include UAM on networks, either internally or external to the organization. This UAM on all classified networks is performed to detect activity indicative of insider threat behavior. Service Level Agreements (SLA) must be executed with agencies that operate or provide classified network connectivity or systems, but do not have the capability to perform UAM. The SLAs will outline the capabilities the provider will employ to identify suspicious user behavior and how that information must be reported to the subscriber's insider threat personnel.

(U) Intelligence Community Policy Initiatives

(U) The IC Standards (ICS) are applicable to each of the 17 IC agencies⁵, 8 of which are located within DoD. The Committee for National Security Systems (CNSS) creates directives which govern each of the departments/agencies with national security systems.

(U) IC Standards

(U//~~FOUO~~) The Office of the Director of National Security (ODNI) mandated the collection of audit data in IC Standard (ICS) 500-27, "Collection and Sharing of Audit Data," June 2, 2011. IC elements must audit information resources within the IC information environment to protect national intelligence, identify threats (including insider threats), detect and deter penetration of IC information resources, reveal

⁵ (U) Office of the Director of National Intelligence, Air Force Intelligence, Army Intelligence, Central Intelligence Agency, Coast Guard Intelligence, Defense Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State, Department of Treasury, Drug Enforcement Agency, Federal Bureau of Investigation, Marine Corps Intelligence, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security Agency, and Navy Intelligence.

misuse, and identify usage trends⁶. The Military Intelligence Services, which are part of the IC, are required to have the capability to collect key strokes and full application content, obtain screen captures, and perform file shadowing for all lawful purposes, to include detecting unauthorized use or disclosure.

(U//~~FOUO~~) The IC issued ICS 700-2, "Use of Audit Data for Insider Threat Detection," June 2, 2011, in order to use the data collected through ICS 500-27 for the insider threat mission. This policy states IC element heads are responsible for ensuring the implementation of appropriate security and CI initiatives to support the identification, apprehension, and, as appropriate, prosecution of those insiders who endanger national security interests. ICS 700-2 states audit data collected pursuant to ICS 500-27 must be used to identify, proactively or retroactively, electronic activity by personnel that may be indicative of an insider threat.

(U//~~FOUO~~) The IC elements must ensure the establishment of automated triggers⁷. Triggers must be capable of detecting insider threats proactively on an ongoing basis, ideally close to real time. Triggers must be developed and applied in a non-discriminatory manner, based on knowledge and experience of the habits, techniques, and tradecraft of persons who misuse access to IC information resources. Triggers will often be specific to the mission activities of a given IC element. When a user activity meets the trigger threshold, an automate alert should prompt an assessment by authorized, subject to rules and procedures defined by the responsible office.

(U) Committee for National Security Systems

(U//~~FOUO~~) The CNSS, which is chaired by the DoD Chief Information Officer, published CNSS Directive (CNSSD) 504, "Directive on Protecting National Security Systems from Insider Threats," on February 4, 2014. This directive requires U.S. Government Executive Branch departments/agencies (D/A), to establish insider threat capabilities

⁶ (U//~~FOUO~~) Military Intelligence Services (INSCOM, ONI, MCIA, and AFISRA) are required to follow this standard because they are a part of the Intelligence Community.

⁷ (U) Triggers are parameters that signify an anomalous event or activity indicative of an Insider threat or other unauthorized use or unauthorized disclosure.

to protect national security systems in accordance with the Presidential Memorandum. The insider threat capabilities these programs are comprised of must ensure that NSS and the national security information are adequately protected from compromise or exploitation by insiders. Many D/As have existing processes, policies, and capabilities to address insider threats, but often they are dispersed throughout the agency and are not coordinated. These capabilities generally include security, information assurance, human resource, and occasionally counterintelligence. These capacities, when synchronized with each other and automated to the greatest extent possible, can more effectively and efficiently prevent, deter, detect, and mitigate insider exploitation of national security systems.

(U//~~FOUO~~) According to CNSSD 504, agencies that lease, own or use national security systems must implement UAM in order to analyze and attribute user behavior. The minimum UAM capabilities required for all Federal Government D/A to protect national security systems and the information on them include capabilities to collect user activity data: key stroke monitoring and full application content (e.g., email chat, data import, data export), obtain screen captures, and perform file shadowing for all lawful purposes. UAM data must be attributed to a specific user. The D/As, however, are encouraged to implement more stringent standards as their missions require and as organizational risk dictates.

(U) CNSSD 504 states that UAM collection must be accomplished by the D/A through the implementation of triggers that monitor user activities on a network. Each D/A must develop and maintain current triggers that reflect the unique environment of the individual D/A. Some of these triggers that could indicate an insider threat event on a national security system include: account change, authentication failure/change, baseline anomaly, excessive activity, evidence tampering, exfiltration, malware, network traffic anomaly, privilege violation, system configuration change, and user behavior anomaly.

(U) Department of Defense Policy Initiatives

(U) Undersecretary of Defense for Intelligence

(U) It is DoD policy that the Military Services monitor and audit information for insider threat detection and mitigation. The DoD Insider Threat Program will gather, integrate, review, assess, and respond to information derived from multiple sources. These data sources will include counterintelligence, security, cybersecurity, civilian and military personnel management, workplace violence anti-terrorism (AT) risk management, law enforcement (LE), the monitoring of user activity on DoD information networks, and other sources as necessary and appropriate to identify, mitigate, and counter insider threats.

(U) The DoD CIO's responsibilities within the DoD Insider Threat Program are to develop and implement policy and strategy, to include audit and UAM standards, to counter insider threats on DoD information networks.

(U) Military Service Insider Threat Policies

(U) The delay in the development and publishing of the DoD Insider Threat Program Directive did not hamper the Military Services' development of their insider threat program policy. The Army, Air Force, and the Department of the Navy published their insider threat program policies prior to the Office of the Undersecretary of Defense for Intelligence's (OUSDI) insider threat directive. The Military Services were able to do this by using the NITTF minimum standards as a guide in the policy development.

(U) U.S. Army

(U) The Department of the Army issued Army Directive 2013-18, "Army Insider Threat Program," on July 31, 2013.

ARMY: (b) (5), (b) (7)(E)

(U) ARMY: (b) (5), (b) (7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(U) ARMY: (b) (5), (b) (7)(E)

[REDACTED]

[REDACTED]

[REDACTED]

(U) U.S. Navy and U.S. Marine Corps

(U) The Department of the Navy (DON) issued Secretary of the Navy Instruction (SECNAVINST) 5510.37, "Department of the Navy Insider Threat Program," on August 8, 2013. This instruction is applicable to both the Navy and the Marine Corps. This instruction dictates that the DON will enhance technical capabilities to monitor user activity on all systems in support of a continuous evaluation.

(U) The DON CIO has to ensure the DON organizations design, develop, deploy, and operate technology-enabled techniques on all DON networks to discover and monitor user activities that may indicate insider threat activity.

(U) The Office of the Chief of Naval Operations (OPNAV) issued OPNAVINST 5510.165, "Navy Insider Threat Program," on January 27, 2015. This instruction, which applies to all Navy personnel, includes planning, programming, and implementing enhanced technical capability to monitor user activity on all Navy networks and systems. The Navy's Information Dominance Directorate (N2/N6) maintains an insider threat to cybersecurity program as the designated Navy lead for insider threat to cyber-based aspects of the Navy InT program. The Office of Naval Intelligence is to serve as the central operational authority for Navy sensitive compartmented information networks.

(U) The U.S. Marine Corps is working on a Marine Corps Order (MCO) for insider threat. The USMC anticipates that the MCO will be ready for coordination for comments by August 2015.

(U) U.S. Air Force

(U) The Department of the Air Force (AF) issued AF Instruction 16-1402, "Insider Threat Program Management," on August 5, 2014. This instruction assigns responsibilities for the oversight and management of the Air Force Insider Threat Program. The Air Force Insider Threat Program will include network monitoring and auditing as one of its focus areas. Available monitoring and auditing capabilities must support insider threat detection and mitigation efforts to the extent possible. Monitoring and auditing capabilities must be integrated into the overall insider threat mitigation process. Capabilities should consistently be improved in order to meet current and future Air Force mission requirements as well as Federal and DoD standards, and to proactively incorporate best practices to prevent and detect anomalous activity.

(U) The AF Director of Security, Special Program Oversight and Information Protection, as the designated representative for insider threat program management and accountability, is also charged with issuing policies and procedures that support monitoring and auditing of SAP networks and assets for insider threat detection and mitigation.

(U) The AF Chief of Information Dominance and CIO issues policies and procedures that support monitoring and auditing of applicable networks and assets to support insider threat deterrence, detection, and mitigation.

(U) The AF Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance is charged with overseeing the monitoring and auditing of AF JWICS networks and assets for insider threat activities. The Deputy Chief also establishes procedures to securely provide insider threat program personnel regular, timely, and electronic access to information necessary to identify, analyze and resolve inside threat issues.

(U) The AF Deputy Chief of Staff for Operations, Plans, and Requirements will ensure cyber space operations support the capability to monitor and audit user activity in accordance with U.S. Cyber Command talking orders.

~~SECRET//NOFORN~~

UNCLASSIFIED//NOFORN

(U) Appendix C

(U) Organizations Visited and Contacted

| |
|---|
| Office of the Secretary of Defense |
| Office of the Under Secretary of Defense for Intelligence |
| Office of the Under Secretary of Defense Comptroller |
| Office of the Chief Information Officer |
| DoD Support Agency |
| Defense Information Systems Agency |
| Military Services |
| U.S. Army |
| U.S. Navy |
| U.S. Air force |
| U.S. Marine Corps |

UNCLASSIFIED//NOFORN

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) Management Comments

(U) Office of the Under Secretary of Defense, Director
for Defense Intelligence (Intelligence & Security)



INTELLIGENCE

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-5000

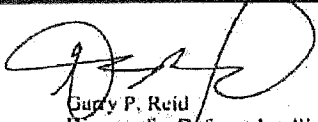
MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
(ATTN: DEPUTY ASSISTANT INSPECTOR GENERAL,
INTELLIGENCE AND SPECIAL PROGRAM ASSESSMENTS-
INTELLIGENCE EVALUATIONS)

SUBJECT: Draft Department of Defense Inspector General Report, "Assessment of the
Military Services' Insider Threat Programs." (Project No. D2014-DINT01-
0043.000)

Thank you for the opportunity to respond to the Inspector General's draft report and
discuss the Department of Defense (DoD) Insider Threat Program with your staff. We are in
agreement with your recommendations and have already taken actions to address them. Please
see our comments of the draft report in the attached.

I would ask that your team reconsider the assessment that OUSD(I) efforts to publish the
DoD insider threat policy were not timely. As your report noted, the USD(I) became the DoD
Senior Official for insider threat in September 2013 and the Deputy Secretary of Defense signed
the DoD insider threat policy in September 2014. Our processing and publication of the
Department's insider threat policy fell within the time standards set by the DoD Directives
Branch, Washington Headquarters Service.

Thanks again for working with us on this important issue. My staff would be happy to
continue discussing this matter with your team. My primary points of contact are


Garry P. Reid
Director for Defense Intelligence
(Intelligence & Security)

Attachment:
As stated

170000 0015 184 140

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) Office of the Under Secretary of Defense, Director
for Defense Intelligence (Intelligence & Security)
(cont'd)

DoD IG Draft Report Dated August 4, 2015
Project No. D2014-DINT01-0043.000

Assessment of the Military Services' Insider Threat Programs

RECOMMENDATION: That the USD(I) establish an insider threat program office which provides for management, accountability, and oversight of the DoD insider threat program.

DoD RESPONSE: Agree. An internal assessment is being conducted to determine the best organizational structure for the DoD insider threat program office, with feedback expected in December 2015. In the interim, OUSD(I) dedicated staff within the Office of the Director for Defense Intelligence (Intelligence and Security) manage the DoD insider threat program at the enterprise level, and placed a DoD liaison officer at the National Insider Threat Task Force. With the addition of two full-time contractors planned for FY 16, the DoD Insider Threat Branch will be better positioned to accomplish the management and oversight functions specified in national and DoD insider threat policies.

RECOMMENDATION: That the USD(I) establish an insider threat program office which makes resource recommendations to the Secretary of Defense by developing a plan to fully fund the DoD insider threat program.

DoD RESPONSE: Agree. As the Principal Staff Assistant for security and insider threat, the USD(I) has included resource recommendations in the current and previous two Program Budget Review cycles. OUSD(I) is also designing the content and scope of the annual status report to the Secretary of Defense and resource recommendations will be a key component of that report. The FY 16-20 program build included funds for critical insider threat efforts supporting the DoD enterprise program; specifically, the DoD Insider Threat Management and Analysis Center and Continuous Evaluation pilots. Additionally, OUSD(I) personnel are reviewing all funding streams that have an insider threat nexus for possible enhancements. OUSD(I) and DoD Components will continue to collaborate on identifying the resources needed, potential sources, and pursuing those actions required to procure them.

RECOMMENDATION: That the USD(I) establish an insider threat program office which develops a DoD level insider threat implementation plan.

DoD RESPONSE: Agree. The DoD implementation plan has been written and coordinated with all DoD Components. Publication of this plan is projected in the first quarter of CY 16.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Do not use for public release

(U) U.S. Army, Deputy Chief of Staff, Director, G-34



~~FOR OFFICIAL USE ONLY~~

DEPARTMENT OF THE ARMY
OFFICE OF THE
DEPUTY CHIEF OF STAFF, G-34
AND ARMY PERS/ASST
HEADQUARTERS, DA, 20315-2000

DAMO-ODP

19AUG15

MEMORANDUM FOR INSPECTOR GENERAL DEPARTMENT OF DEFENSE (ATTN: [REDACTED])

SUBJECT: Army Response to DOD IG Assessment of the Military Services' Insider Threat Programs

1. This memorandum serves as an official response to the DOD IG Assessment of the Military Services' Insider Threat Programs as requested on 5AUG15 with a suspense of 19AUG15. ARMY: (b) (5), (b) (7)(E)

[REDACTED]

2. (U//FOUO) ARMY: (b) (5), (b) (7)(E)

[REDACTED]

3. (U) ARMY: (b) (5), (b) (7)(E)

[REDACTED]

~~FOR OFFICIAL USE ONLY~~

Do not use for public release

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) U.S. Army, Deputy Chief of Staff, Director, G-34
(cont'd)

~~FOR OFFICIAL USE ONLY~~

DAMO-ODP

SUBJECT: Army Response to DOD IG Assessment of the Military Services' Insider Threat Programs

4. (U) ARMY: (b) (5), (b) (7)(E)



5. Army POC for this action is




MICHAEL R. SMITH
Major General, GS
Director, G-34

~~FOR OFFICIAL USE ONLY~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

14-00000 14-00000

(U) U.S. Navy, Staff of Chief of Naval Operations

~~SECRET//NOFORN~~
INFO MEMO

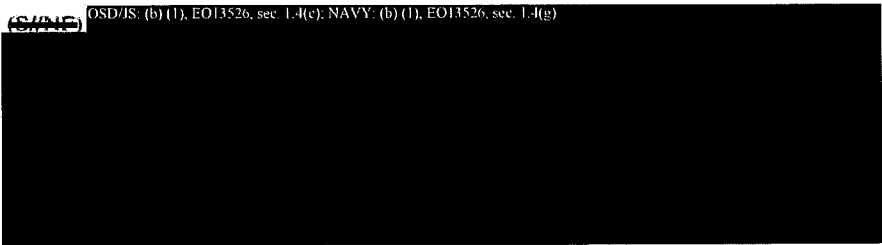
August 27, 2015

FOR: DEPARTMENT OF DEFENSE, INSPECTOR GENERAL

FROM: VADM R. R. Braun, Director, Navy Staff

SUBJECT: DoD IG Assessment of the Military Services' Insider Threat Programs (U)

- (U) The Chief of Naval Operations (CNO) was requested to provide comments on the DoD IG Assessment of the Military Services' Insider Threat Programs (InTPs). The major report finding is that the Military Services are not yet fully compliant with the Insider Threat Minimum Standards. The Military Services InT program lack implementation guidance from the DoD-level Insider threat senior official and consistent DoD-level Insider Threat program resources.

- (S//NF) OSD/JS: (b) (1), EO13526, sec. 1.4(c); NAVY: (b) (1), EO13526, sec. 1.4(g)
- 

- Navy concurs with the report's major finding.
- Attached is a list of planned or completed Navy actions that address the DoD IG's compiled recommendations.

ATTACHMENTS:

As stated

Derived from: NITTF SCG V1.0

Declassify on: 25 Aug 2040

Prepared by 

~~SECRET//NOFORN~~
14-00000 14-00000

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) U.S. Navy, Staff of Chief of Naval Operations
(cont'd)

ATTACHMENT 1

August 27, 2015

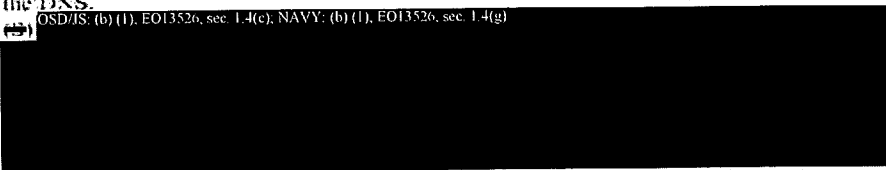
SUBJECT: Planned and/or Completed Navy actions that address the DoD IG's compiled recommendations ~~(S//NF)~~

RECOMMENDATION 2:

(U) Establish an Insider Threat Office of Primary Responsibility to execute the responsibilities stated in the minimum standards and in DoDD 5205.16.

- o (U) OPNAV concurs with recommendation.
- o (U) OPNAV designated a Senior Official for the Navy and an office of primary responsibility for Insider Threat. The Director of Navy Staff (DNS) executes oversight and management of the Navy's Insider Threat Program. The DNS directs Navy capability, resource planning and programing efforts to effectively detect, deter and mitigate insider threats in compliance with the minimum standards and the DoD 5205.16.
- o (U) The Deputy Chief of Naval Operations (DCNO), Information Dominance (N2N6), established the Insider Threat to Cyber Security Office to develop and plan an automated insider threat analytic and response capability to review and respond to information derived from anomaly detection, continuous evaluation, and other sources as necessary.

SUB-RECOMMENDATION:

- a. (U) Implement the user activity monitoring aspect of the Minimum Standards for Executive Branch Insider Threat Programs on all classified networks.
 - o (U) OPNAV concurs with recommendation.
 - o (U) The DCNO (N2N6) established an Insider Threat to Cyber Security Office to coordinate and manage anomaly detection, information assurance and cyber in support of the DNS.
 - o ~~(S)~~ OSD/JS: (b) (1), EO13526, sec. 1.4(c); NAVY: (b) (1), EO13526, sec. 1.4(g)

 - o (U/~~FOUO~~) In July 2015, The Space and Warfare Systems Command (SPAWAR) provided the NITBOG a Navy InT to Cyber Security analysis, which recommended new or modified controls and associated architecture revisions, along with broad resource and manpower requirements, to expand UAM coverage to all networks. The DNS Insider

~~SECRET//NOFORN~~

(U) U.S. Navy, Staff of Chief of Naval Operations
(cont'd)

SECRET//NOFORN

Threat Working Group is developing an acquisition strategy, resource requirements, and an implementation plan to expand UAM coverage to SIPR in FY 18.

- o ~~(U//FOUO)~~ OSD/JS: (b) (1), EO13526, sec. 1.4(c); NAVY: (b) (1), EO13526, sec. 1.4(g)

- e. (U) Establish an InT implementation plan.
 - o (U) OPNAV concurs with recommendation.
 - o (U) In June 2015, The DNS drafted an InT Implementation Plan that is in formal policy coordination for review and comment.
 - d. (U) Monitor and report progress on the implementation of their insider threat programs.
 - o (U) OPNAV concurs with recommendation.
 - o (U//FOUO) In October 2015, the DNS will oversee the preparation of an annual report, for delivery to the CNO, which provides an update on the completion of requirements found in the InT Implementation Plan, additional accomplishments, resources allocated, insider threats risks identified, recommendations, goals for Program improvement, and that identifies major impediments or challenges. Further, DNS will provide programming recommendations to CNO for Navy Insider Threat.
 - o (U) The DNS will facilitate reviews of the Navy's InT program to ensure compliance with policy guidance, including a requirement to conduct and report of self-assessments.
 - e. (U) Identify internal funding requirements in a program objective memorandum to USD(H).
 - o (U) OPNAV concurs with recommendation.
 - o (U) DNS established the Navy Insider Threat Board of Governance (NITBOG) to provide senior leadership recommended actions, prioritization, planning, programming, information sharing and execution of activities in support of a comprehensive Navy InTP.
 - o (U//FOUO) In July 2015, SPAWAR provided the NITBOG a Navy InT to Cyber Security analysis, which defined and documented existing gaps in InT to Cyber Security controls, and recommended new or modified controls and associated architecture revisions, along with broad resource and manpower requirements, to ensure U.S. Navy meets insider threat program requirements.
- (U) The NITBOG will develop InT resource recommendations for the DNS to present to CNO and CUSDI for FY18 POM.

SECRET//NOFORN

~~SECRET//NOFORN~~

(U) U.S. Air Force, Chief of Staff



Office Of The Secretary

CLASSIFICATION: UNCLASSIFIED
DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

SEP 8 2015

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: HQ USAF-CC
1670 Air Force Pentagon
Washington, DC 20330-1670

SUBJECT: Department of Defense Inspector General (DoDIG) Draft Report, Assessment of the Military Services' Insider Threat (InT) Programs

~~(FOUO)~~ We reviewed the report with regards to Recommendation 2a, c, d, and e:

a. ~~(U//FOUO)~~ Implement User Activity Monitoring (UAM) aspect of the Minimum Standards for Executive Branch Insider Threat Programs on all classified networks. *The Air Force agrees with this recommendation. The Air Force completed a requirement gap analysis for implementing UAM on all classified networks which identified funding requirements to expand UAM to Special Access Programs and SIPR. This requirement is competing for funding in FY15, pending the outcome of reprogramming actions currently in Congress. The Air Force has implemented UAM on portions of the classified network fabric and expects to fully meet the classified network requirement in FY16. The Air Force Security Enterprise Executive Board (AFSEEB) will review status in September and we will fund UAM to the appropriate amounts in accordance with requirements, threat assessments, and competing priorities. We will use the FY17 PBR and the FY18 POM to implement any funding adjustments.*

c. (U) Establish an InT implementation plan. *The Air Force agrees with this recommendation. The Air Force completed final functional coordination of its InT Implementation Plan on 9 August 2015 and expects final publication by 4 September 2015.*

d. (U) Monitor and report progress on the implementation of their Insider threat programs. *The Air Force agrees with this recommendation. The Air Force reported initial task completion to National Insider Threat Task Force (NITTF) on 26 June 2014 and is scheduled for an assessment by the NITTF on 2 December 2015. The AFSEEB, which includes senior-level participation from the intelligence, security forces, acquisition, inspector general, communications, operations, personnel, and nuclear enterprise communities, meets monthly to review InT implementation and work evolving issues.*

CLASSIFICATION: UNCLASSIFIED

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

1. *Chlorophyll a* and *Chlorophyll b* contents were determined by spectrophotometry using the method of Lichtenthaler and Whistler (1987).

U.S. Air Force, Chief of Staff (cont'd)

CLASSIFICATION: UNCLASSIFIED

e. (U) Identify internal InT funding requirements in a program objective memorandum (POM) to USD(I). *The Air Force agrees with this recommendation. The Air Force completed a cross functional requirement gap analysis on 11 August 2015. The Air Force will address funding in the FY18 POM.*

Please contact

DOD OIG: (b) (6)

Administrative Assistant

CLASSIFICATION: UNCLASSIFIED

1949-1950-1951

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) U.S. Marine Corps, Assistant Deputy Commandant,
Plans, Policies, and Operations (Security)



~~SECRET//NOFORN~~
DEPARTMENT OF THE NAVY
HEADQUARTERS US MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, D.C. 20380-0000

1500
PS

15 SEP 2015

[REDACTED]
Deputy Assistant Inspector General
ISPA-Intelligence Evaluations

(U) This is the United States Marine Corps (USMC) response to the Deputy Assistant Inspector General, ISPA-Intelligence Evaluations Memorandum, SUBJECT: Assessment of the Military Services' Insider Threat Programs (U) dated 04 August, 2015. (Project No. D2014-DINT01-0043.000)

(U) USMC comments to the Recommendations Requiring Comment (2.a, 2.b, 2.c, 2.d, 2.e), outlined in the Department of Defense Inspector General's Results in Brief, are attached. The overall lead for this effort is Security Branch within Security Division. The primary point of contact [REDACTED]

The alternate POC is [REDACTED]

A handwritten signature in black ink, appearing to read "JAM M. Durham".

JAM M. DURHAM
Assistant Deputy Commandant Plans,
Policies, and Operations (Security)
Acting

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

WJ 042550 34 31 000000000000

(U) U.S. Marine Corps, Assistant Deputy Commandant,
Plans, Policies, and Operations (Security) (cont'd)

~~SECRET~~

Department of Defense Inspector General Results in Brief
(Project No. D2014-DINT01-0043.000) (S//NF)

Assessment of the Military Services' Insider Threat Programs (U)

(U) Recommendation #2a: Implement the DoD OIG (b)(5), (b)(7)(E)

(U) USMC Response: CONCUR. Current UAM (and audit) is being conducted at the Marine Corps Intelligence Activity (MCIA) for DoD OIG: (b)(5), (b)(7)(E)

- Marine Corps Systems Command (MCSC) is deploying a Host Based Security System (HBSS) Data Loss Prevention (DLP) capability. DoD OIG, (b)(5), (b)(7)(E) [REDACTED]
- Three DLP pilots have been completed by Marine Corps Command, Control, Communications, and Computer (C4) and MCSC.
- MARFORCYBER is creating an Urgent Needs Statement (UNS) to procure a significant amount of storage capability to better support data and user auditing requirements.

Note: During August 2015, C4 and MARFORCYBER initiated an analysis/study, led by the Carnegie Mellon computer emergency response team (CERT) to assess the current areas where the Marine Corps is currently doing Insider Threat functions and DLP activities. DoD OIG: (b)(5), (b)(7)(E)
DoD OIG: (b)(5), (b)(7)(E)



[illegible]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Page 6 of 10 (10-17-15)

(U) U.S. Marine Corps, Assistant Deputy Commandant,
Plans, Policies, and Operations (Security) (cont'd)

~~SECRET//NOFORN~~

**Department of Defense Inspector General Results in Brief
(Project No. D2014-DINT01-0043.000) (S//NF)**

Assessment of the Military Services' Insider Threat Programs (U)

(U) Recommendation #2b: Establish an Insider Threat Program policy.

(U) USMC Response: CONCUR. Current policy for the Marine Corps Insider Threat Program was promulgated on 10 April, 2015 via MARADMIN 187/15 with the focus on intervention and the prevention of threats which may result in damage or destruction to Marine Corps persons, places, and things. A supporting Marine Corps Order (MCO) is currently being drafted which will include the recent revisions to the Department of Defense (DoD) Insider Threat policy. The estimated signature date for the MCO is 3rd Quarter FY16.

(U) Recommendation #2c: Establish an Insider Threat Implementation Plan.

(U) USMC Response: CONCUR. Concurrently with the drafting of the supporting MCO, an implementation plan is currently being drafted. The estimated signature date for the implementation plan is 3rd Quarter FY16.

Note: An Insider Threat Functional Area Checklist is under development and will be posted on the Inspector General of the Marine Corps Inspection Division web-site when completed. The estimated completion is estimated during 3rd Quarter FY16.

(U) Recommendation #2d: Monitor and report progress on the implementation of their Insider Threat Programs.

(U) USMC Response: CONCUR. Security Branch is currently providing oversight, to include reporting and monitoring, for the development and expansion of the Marine Corps Insider Threat Program.

Note: To mitigate the Insider Threat and protect the total force, the Marine Corps has drafted an initiative to establish a Marine Corps Insider Threat Management and Analysis Center (MCITMAC) to integrate and centrally analyze key threat-related information on potential Insider Threats who may pose a risk to

3
~~SECRET//NOFORN~~

Page 6 of 10 (10-17-15)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Working Draft Document

(U) U.S. Marine Corps, Assistant Deputy Commandant,
Plans, Policies, and Operations (Security) (cont'd)

~~SECRET//NOFORN~~

**Department of Defense Inspector General Results in Brief
(Project No. D2014-DERT01-0043.000) (S//NF)**

Assessment of the Military Services' Insider Threat Programs (U)

personnel, facilities, networks, and national security information. The MCITMAC will analyze information and data derived from NIPR, SIPR, and OWICS networks. The MCITMAC will collect and distribute Insider Threat information across the enterprise and collaborate closely with the Department of Defense Insider Threat Management and Analysis Center (DITMAC). The Initial Operational Capability (IOC) for the MCITMAC is scheduled for 1st Quarter FY16 (this is in line with the DITMAC IOC).

Additional Information: The Marine Corps has initiated discussions with the Department of the Navy (DoN) Chief of Security Enterprises on the feasibility of establishing a Navy and Marine Corps Insider Threat Management and Analysis Center.

(U) Recommendation #2e: Identify internal Insider Threat funding requirements in a Program Objective Memorandum (POM) to OSD(I).

(U) USMC Response: CONCUR. Current Insider Threat requirements are being entered into the Marine Corps Capability Based Assessment (MC-CBA) process. This process includes capabilities, gap, solutions, and risk analyses. The information derived from this process will inform the investment strategies for the next POM cycle. The estimated completion date for the Capabilities Investment Plan (CIP) submission is 4th Quarter FY16.

Note from C4 SME: "We cannot move forward with an acquisition strategy or attempt to engineer or integrate more capability on top of what already exists in the Marine Corps Enterprise Secret Network (a network of networks) (MCEN-S) until we have done a thorough analysis, and have a clear understanding of the true gaps. The Marine Corps has existing capability and technology in place performing a number of DLP and Continuous Monitoring (CM) and audit/management features, and we would like to utilize existing capabilities where possible. We are doing our due diligence with the analysis before putting together a Business Cost Analysis (BCA) and ask for more funding for C4. Based on the information we have today, we believe significant funding will be required to meet each objective conclusively." The

~~SECRET//NOFORN~~

Working Draft Document

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Page 2 of 10

(U) U.S. Marine Corps, Assistant Deputy Commandant,
Plans, Policies, and Operations (Security) (cont'd)

~~SECRET//NOFORN~~

Department of Defense Inspector General Results in Brief
(Project No. D2014-DINT01-0043.000) (S//NF)

Assessment of the Military Services' Insider Threat Programs (U)

estimated completion date for the analysis and BAC submission is
2nd Quarter FY16.

Note from Security Branch Head: "We are currently involved with
the Cost Assessment and Program Evaluation (CAPE) Director,
specifically the Insider Threat Issue Team, where we are
developing cost estimations for the Insider Threat requirements
across the Fiscal Year Defense Plan (FYDP). Our initial
submission is due to the CAPE during 1st Quarter FY16."

CLASSIFIED BY: [REDACTED]

REASON: Derived from multiple sources
DECLASSIFY ON: March, 12, 2039

5

~~SECRET//NOFORN~~

DDI-2014-01-03

~~SECRET//NOFORN~~

(U) Acronyms and Abbreviations

| | |
|-----------------|---|
| AFRISA | Air Force Intelligence, Surveillance, and Reconnaissance Agency |
| AJNAP | Army JWICS Network Audit Program |
| CAP | Controlled Access Program |
| CIO | Chief Information Officer |
| DISA | Defense Information Systems Agency |
| DNI | Director of National Information |
| D/A | Departments and Agencies |
| E.O. | Executive Order |
| GISA | Ground Intelligence Support Agency |
| HBSS | Host Based Security Suite |
| IAR | Incident Assessment Report |
| ICS | Intelligence Community Standard |
| InT | Insider Threat |
| JWICS | Joint Worldwide Intelligence Community System |
| MCIA | Marine Corps Intelligence Activity |
| NIP | National Intelligence Program |
| NIPRNET | Non-secure Internet Protocol Router Network |
| NITTF | National Insider Threat Task Force |
| DON | Department of the Navy |
| ODNI | Office of the Director for National Intelligence |
| ONI | Office of National Intelligence |
| OSD | Office of the Secretary of Defense |
| OUSD(C) | Office of the Under Secretary of Defense for Comptroller |
| OUSD(I) | Office of the Under Secretary of Defense for Intelligence |
| PP&O | Plans, Policy, and Operations |
| PPOI | Plans, Policy, Oversight and Integration |
| SAF/AAZE | Policy and Security Enterprise Division |

~~SECRET//NOFORN~~

SAP Special Access Program
SAPCO Special Access Program Central Office
SCC Security Coordination Center
SIPRNET Secret Internet Protocol Router Network
SME Subject Matter Expert
UAM User Activity Monitoring
USD(I) Under Secretary of Defense for Intelligence
USMC United States Marine Corps

~~SECRET//NOFORN~~

Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD IG Director for Whistleblowing & Transparency. For more information on your rights and remedies against retaliation, go to the Whistleblower webpage at www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison

703.604.8324

DoD Hotline

800.424.9098

Media Contact

Public.Affairs@dodig.mil; 703.604.8324

Monthly Update

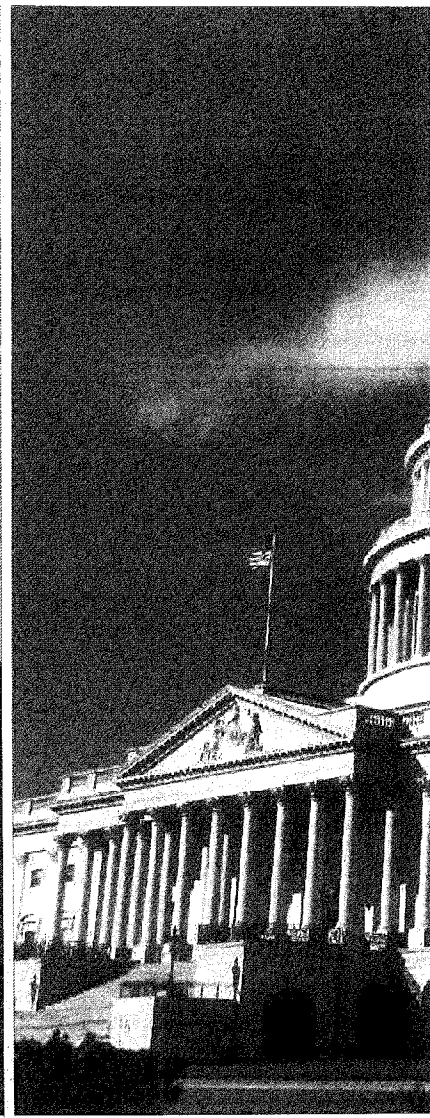
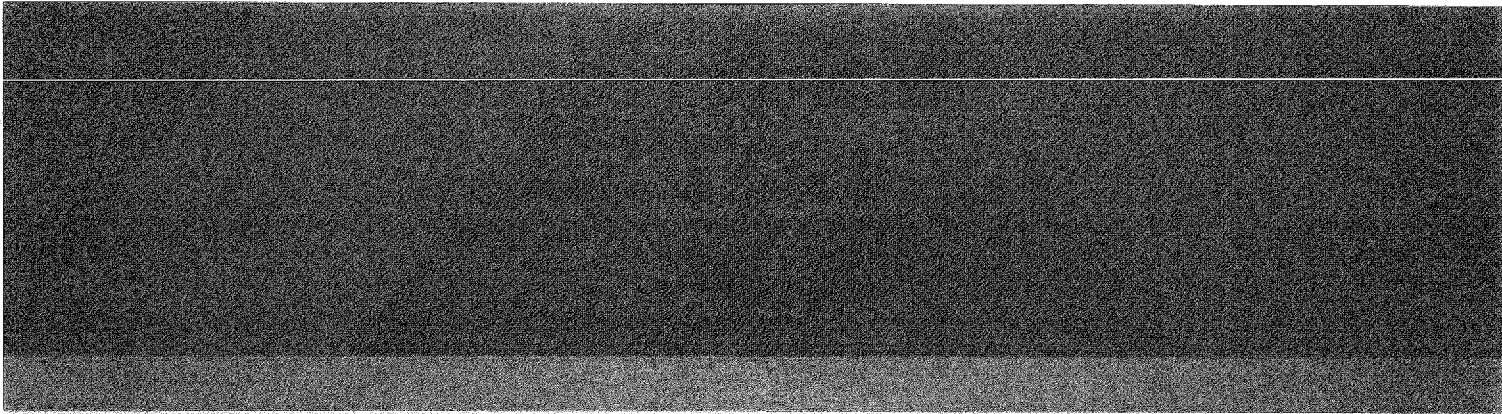
dodigconnect-request@listserve.com

Reports Mailing List

dodig_report-request@listserve.com

Twitter

twitter.com/DoD_IG



Department of Defense | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.1500

