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

September 12, 2018
Ref: FOIA-2015-00203

SENT VIA EMAIL TO: 14878-99862718@requests.muckrock.com
Mr. Shawn Musgrave
MuckRock News
DEPT MR 14878
P.O. Box 55819
Boston, MA 02205-5819

Dear Mr. Musgrave:

This is in response to your Freedom of Information Act (FOIA) request for a copy of DODIG-2015-046, "Navy Commands Need to Improve Logical and Physical Controls Protecting SIPRNET Access Points." We received your request on December 19, 2014, and assigned it case number FOIA-2015-00203.

The Office of the Deputy Inspector General for Audit conducted a search and located one document, totaling 90 pages, which is responsive to your request. Upon review, we determined that certain redacted portions are exempt from release pursuant to 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, the Department of the Navy reviewed the report and determined that further redacted portions are exempt from release in accordance with 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(g) (vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security).

If you consider this response to be an adverse determination, you may submit an appeal. You can appeal in writing to the Department of Defense, Office of Inspector General, ATTN: FOIA Appellate Authority, Suite 10B24, 4800 Mark Center Drive, Alexandria, VA 22350-1500. Any appeal must be postmarked within 90 days of the date of this letter, must clearly state the adverse determination being appealed, and should reference the file number above. We recommend that your appeal and its envelope both bear the notation "Freedom of Information Act Appeal." For more information on appellate matters and procedures, please refer to 32 C.F.R. Sec. 286.9(e) and 286.11(a) for further information on administrative appeals.

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/. You may also contact OGIS via regular mail at National Archives and Records Administration Office of Government Information Services, 8601 Adelphi Road – OGIS, College Park, MD 20740-6001. 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 Searle Slutzkin 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

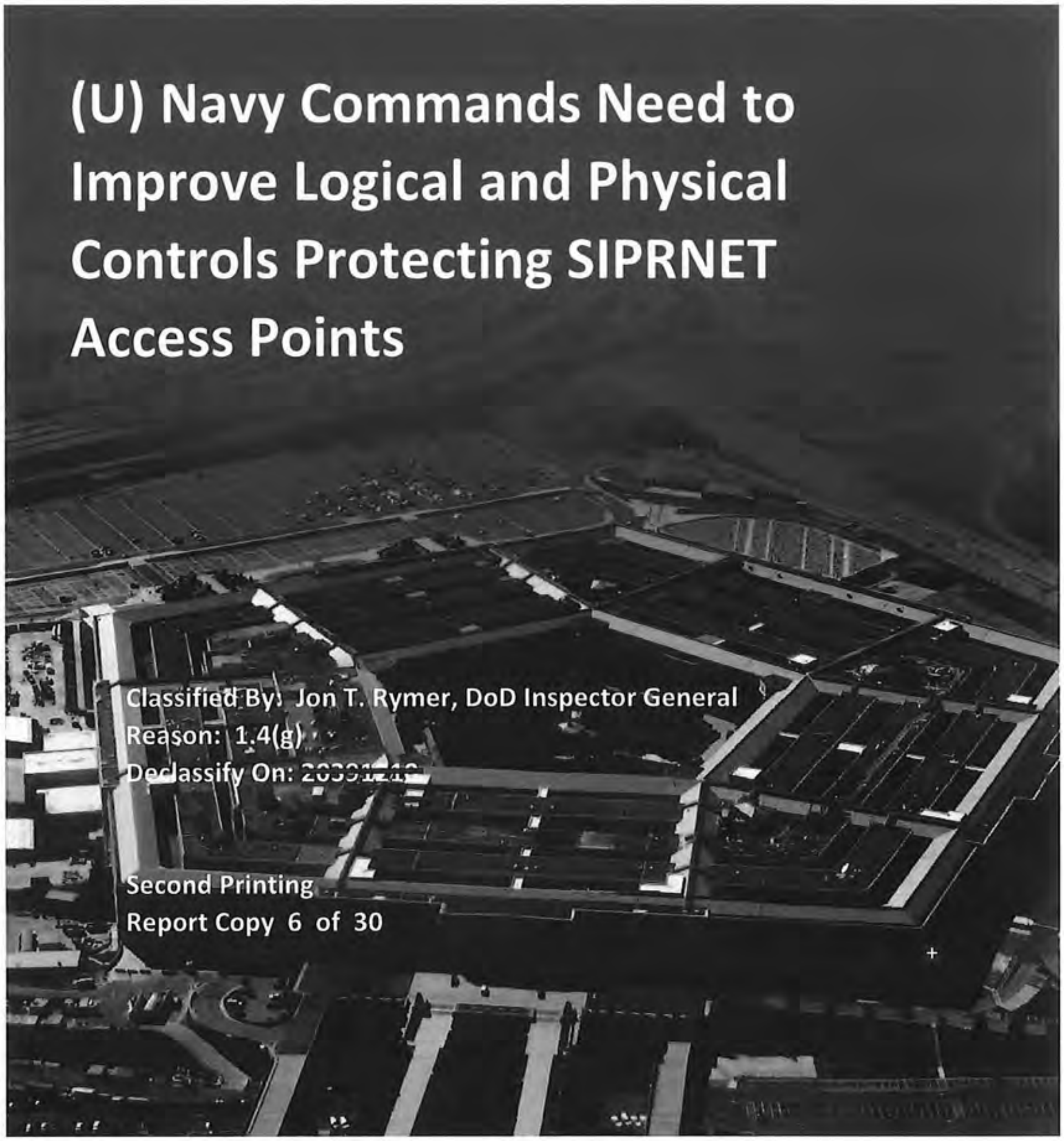
Report No. DODIG-2015-046

~~SECRET~~

INSPECTOR GENERAL

U.S. Department of Defense

December 10, 2014



(U) Navy Commands Need to Improve Logical and Physical Controls Protecting SIPRNET Access Points

Classified By: Jon T. Rymer, DoD Inspector General
Reason: 1.4(g)
Declassify On: ~~20391210~~

Second Printing
Report Copy 6 of 30

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~SECRET~~

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|800.424.9098

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

Results in Brief

Navy Commands Need to Improve Logical and Physical Controls Protecting SIPRNET Access Points

December 10, 2014

(U) Objective

(U) Our objective was to determine whether the Navy was effectively protecting its Secret Internet Protocol Router Network (SIPRNET) access points. Specifically, we reviewed the logical and physical controls protecting the SIPRNET access points at DoDIG: (b)(7)(E).

(U) Findings

(~~S~~) NAVY: (b)(1), Sec. 1.4(g)

(~~FOUO~~) DoDIG: (b)(7)(E)

(U) Findings (cont'd)

(~~FOUO~~) DoDIG: (b)(7)(E)

(U) Recommendations

(~~S~~) NAVY: (b)(1), Sec. 1.4(g)

(~~FOUO~~) DoDIG: (b)(7)(E)

(U) Management Comments and Our Response

(~~FOUO~~) We renumbered two recommendations for Finding A. Generally, management comments addressed the specifics of our recommendations. However, we request that the Under Secretary of Defense for Intelligence; Commander, U.S. Cyber Command; DoDIG: (b)(7)(E) provide additional comments in response to this report. In addition, we received the DoD CIO comments on the draft report too late to include them in the final report. Therefore, if the DoD CIO does not submit additional comments, we will consider those comments as the management response to the final report. Please see the Recommendations Table on the back of this page.

(U) Recommendations Table

(U) Management	Recommendations Requiring Comment	No Additional Comments Required
Under Secretary of Defense for Intelligence	A.1	
Commander, U.S. Cyber Command	A.1	A.2
Deputy Under Secretary of the Navy, Policy		A.3
Department of Defense Chief Information Officer	A.1	
Department of the Navy Chief Information Officer		A.4
Department of the Navy Deputy Chief Information Officer (Navy)		A.4, A.5.a, A.5.b, B.1, B.2
Commander, U.S. Fleet Cyber Command/U.S. Tenth Fleet		B.1
DoDIG: (b)(7)(E) [redacted]		A.6, A.7.a, A.7.b, A.7.c, A.8.a, A.8.b
DoDIG: (b)(7)(E) [redacted]		A.8.a, A.8.b
DoDIG: (b)(7)(E) [redacted]		A.6, A.7.a, A.7.b, A.7.c
DoDIG: (b)(7)(E) [redacted]	A.9.a, A.9.c	A.9.b
DoDIG: (b)(7)(E) [redacted]		A.10, B.4
Director, Navy Operational Designated Accrediting Authority		B.3.a, B.3.b, B.3.c, B.3.d, B.3.e, B.4
DoDIG: (b)(7)(E) [redacted]	A.6	A.8.a, A.8.b
DoDIG: (b)(7)(E) [redacted]	A.11.b, A.11.d, A.11.e	A.7.a, A.7.b, A.7.c, A.11.a, A.11.c (U)

(U) Please provide Management Comments by January 12, 2015.

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

December 10, 2014

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
COMMANDER, U.S. CYBER COMMAND
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
NAVAL INSPECTOR GENERAL

SUBJECT: Navy Commands Need to Improve Logical and Physical Controls Protecting SIPRNET Access Points (Report No. DODIG-2015-046)

~~(FOUO)~~ We are providing this report for your review and comment. DoDIG (b)(7)(E)

(U) We considered management comments on a draft of this report when preparing the final report. DoD Directive 7650.3 requires that recommendations be resolved promptly. Comments from the Under Secretary of Defense for Intelligence, and the Commander, U.S. Cyber Command partially addressed Recommendation A.1. Therefore, we request additional comments on this recommendation by January 12, 2015. Comments from DoDIG (b)(7)(E) did not address Recommendation A.6. Therefore, we request additional comments on this recommendation by January 12, 2015. Comments from the DoDIG (b)(7)(E) partially addressed Recommendations A.9.a and A.9.c. Therefore, we request additional comments on these recommendations by January 12, 2015. Comments from the DoDIG (b)(7)(E) partially addressed Recommendations A.11.b, A.11.d, and A.11.e. Therefore, we request additional comments on these recommendations by January 12, 2015. We received the DoD Chief Information Officer comments on the draft report too late to include them in the final report. Therefore, if the DoD Chief Information Officer does not submit additional comments, we will consider those comments as the management response to the final report.

(U) Please send a PDF file containing your comments to DoDIG (b)(6) @dodig.smil.mil and DoDIG (b)(6) @dodig.smil.mil. Copies of your comments must have the actual signature of the

(U) authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified documents electronically, you must send them over the SIPRNET.

(U) We appreciate the courtesies extended to the staff. Please direct questions to DoDIG (b)(6) at (703) 604DoDIG (b)(6) (DSN 664DoDIG (b)(6) or DoDIG (b)(6) at (703) 601DoDIG (b)(6) (DSN 329DoDIG (b)(6).

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

(U) Contents

(U) Introduction

(U) Objective

(U) Our objective was to determine whether the Navy was effectively protecting its Secret Internet Protocol Router Network (SIPRNET) access points. Specifically, we reviewed the logical and physical controls protecting the SIPRNET access points at DoDIG (b)(7)(E) [redacted]. For Scope and Methodology, see Appendix A.

(U) Background

~~(FOUO)~~ The SIPRNET is the Navy's command and control[1] network that operates at the classified Secret level. SIPRNET access points are all possible physical or logical connections where a user can access the SIPRNET. Physical controls, such as locks, guards, and window blinds, deter or delay adversaries' access to the network. Logical controls are system-based mechanisms (for example, firewalls, permission settings, and usernames and passwords) used to designate who or what has access to a specific system or function.

~~(FOUO)~~ The Department of the Navy's (DON) shore-based enterprise network in the continental United States and Hawaii is the Navy Marine Corps Intranet (NMCI), comprising two networks, one that connects to the SIPRNET[2] and one that connects to the Non-secure Internet Protocol Router Network, which is the unclassified network. The NMCI SIPRNET has:

- (U) approximately 77,395 users;
- ~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]
- ~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

~~(FOUO)~~ [1] Command and control means that the Navy uses the network to send operational orders and battle commands to Navy combat forces.

(U) [2] The SIPRNET connects to the Defense Information Systems Network, which is the responsibility of the Defense Information Systems Agency.

(U) [3] A server farm is a collection of servers that are used to route network traffic between two points; in this case, the SIPRNET and Navy installations.

(U) Naval Network Warfare Command (NNWC) is responsible for managing NMCI; however the network is owned and operated by Hewlett Packard Enterprise Services. Currently, Hewlett Packard Enterprise Services works under a continuity contract, which was awarded in October 2010 and is expected to expire in September 2014. Contractor responsibilities include, but are not limited to:

- (U) conducting certification and accreditation testing in accordance with the DoD Information Assurance Certification and Accreditation Process (DIACAP) Implementation Plan and other Government-approved test plans; and
- (U) defending systems by recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies to ensure no uncontrolled access and that all systems and networks can defend themselves.

(U) We reviewed controls at the DoDIG (b)(7)(E) [redacted] use NMCI to connect to the SIPRNET.

(U) Information System Certification and Accreditation

(U) DoD requires that networks be certified and accredited before connecting to the SIPRNET. DoDIG (b)(7)(E) [redacted] was accredited in October 2012 in accordance with DoD Instruction (DoDI) 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007. For more information on DIACAP, see Appendix B. We focused on three DIACAP activities: validation of information assurance (IA) controls, certification and accreditation decisions, and maintaining authorization.

- (U) Validation is the testing, evaluation, examination, and investigation of evidence that assigned IA controls[5] are implemented correctly and effectively.

(~~FOUO~~) [4] We reviewed the logical and physical controls for the Navy Marine Corps Intranet DoDIG (b)(7)(E) [redacted] Classified Transport Boundary, known generically in this report as the DoDIG [redacted] SIPRNET.

(U) [5] IA controls are applied to information systems to achieve an acceptable level of integrity, availability, and confidentiality.

- (U) The certification decision is a determination of the extent to which a system complies with assigned IA controls. The decision is based on validation results that identify and assess the residual risk[6] and the costs to correct or mitigate IA vulnerabilities as documented in the Information Technology (IT) Security Plan of Action and Milestones (POA&M). A certification determination is required before an accreditation decision.
- (U) The accreditation decision is a formal statement by a designated accrediting authority regarding acceptance of the risk associated with operating a DoD information system. The accreditation decision is expressed as an Authorization to Operate (ATO), an Interim ATO, an Interim Authorization to Test, or a Denial of ATO. The Navy Operational Designated Accrediting Authority (ODAA) is the designated accrediting authority for the Navy.
- (U) Maintaining the authorization involves the sustainment of an acceptable security posture. The IA controls should be reviewed annually to confirm their effectiveness or to recommend changes to the accreditation status. The results of an annual review or a major change in information assurance posture at any time may indicate the need for recertification and reaccreditation.

(U) DIACAP requires that all vulnerabilities identified during IA control validation be corrected or mitigated, or that the risk be accepted. In addition, DoD Components are required to report vulnerabilities on the IT Security POA&M before granting an approved accreditation decision for a particular DoD network. The IT Security POA&M assists agencies in identifying, assessing, prioritizing, and monitoring the DoD network's vulnerabilities, and should include the actions performed to correct or mitigate the vulnerabilities. The IT Security POA&M should include the vulnerability, the corresponding unique IA control number, and an assigned vulnerability severity category (CAT):

- (U) CAT I vulnerabilities are assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel and are required to be corrected before an ATO is granted.

(U) [6] Residual risk is the portion of risk remaining after security measures have been applied.

- (U) CAT II vulnerabilities can lead to unauthorized system access or activity, and are required to be corrected or mitigated within 180 days of granting an ATO. If vulnerabilities are not corrected or mitigated within the specified time frame, the ATO becomes invalid.
- (U) CAT III vulnerabilities may impact security posture but are not required to be mitigated or corrected in order for an ATO to be granted.

(U) For more information on IA controls, see Appendix C.

(U) Review of Internal Controls

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

~~(FOUO)~~ We also identified internal control weaknesses for the ODAA. DoDIG: (b)(7)(E) [redacted] We will provide a copy of this report to the senior official responsible for internal controls at ODAA.

(U) Finding A

(U) Navy Commands Did Not Effectively Protect SIPRNET Access Points

(~~FOUO~~) DoDIG: (b)(7)(E) [redacted] Specifically:

- (~~S~~) NAVY: (b)(1), Sec. 1.4(g) [redacted]
- (~~FOUO~~) DoDIG: (b)(7)(E) [redacted]
- (~~FOUO~~) DoDIG: (b)(7)(E) [redacted]
- (~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

(~~FOUO~~) [7] Removable media is defined as compact disc, digital video disc, Secure Digital cards, tape, flash memory data storage devices, MultiMediaCards, removable hard drives, etc.

- ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

- ~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]
- ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]
- ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

[redacted]

(U) [8] DoDIG: (b)(6), (b)(7)(E) [redacted]

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

~~(FOUO)~~ [9] DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ [10] DoDIG: (b)(7)(E) [redacted]

(U) [11] The OSD Memorandum "Insider Treat Mitigation," was signed by the Department of Defense, Chief Information Officer and the Under Secretary of Defense for Intelligence; however, U.S. Cyber Command is responsible for issuing additional guidance.

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

(U) [12] DoDIG: (b)(7)(E) [redacted]

(U) [13] DoDI 8500.01 identifies required security controls, DoDIG: (b)(7)(E) [redacted] that are published in the Knowledge Service, as referenced within this Instruction.

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

- ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]
- ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]
- ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]
- ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]
- ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ The Secretary of the Navy Manual 5510.36, "Department of the Navy Information Security Program," June 2006, needs to be updated to include current DoD requirements. The Manual requires that a classified information storage risk assessment be performed. However, after the Manual was issued, DoD issued DoDM 5200.01, volume 3, which includes minimum requirements that are not outlined in Secretary of the Navy Manual 5510.36. The Deputy Under Secretary of the Navy, Policy, should update DON policy to implement at least the minimum requirements for performing a risk assessment as required by DoDM 5200.01, volume 3. DDCIO(N) should implement the requirements for performing a risk assessment in accordance with updated DON policy and DoDM 5200.01, volume 3.

~~(FOUO)~~ System Access Forms Were Not Appropriately Completed or Approved

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted] did not appropriately complete and approve network access forms before granting access to the SIPRNET. The Navy requires each user requesting system access to have a completed:

- ~~(FOUO)~~ System Access Authorization Request Navy (SAAR-N) form in accordance with Navy Telecommunications Directive 10-11, "OPNAV Form 5239-14/System Access Authorization Request Navy (SAAR-N), October 2011," and
- ~~(FOUO)~~ DD Form 2842 "Department of Defense Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities"[14] to acknowledge their responsibilities of receiving a SIPRNET token.

(U) [14] The DD Form 2842 is used to acknowledge user acceptance of their responsibilities upon receiving their SIPRNET token. The DD Form 2842 requires that the registration official witness the user sign the document.

~~(FOUO)~~ The SAAR-N is used to authorize access to DoD networks. Secretary of the Navy Instruction 5239.3B, "Department of the Navy Information Assurance Policy," June 17, 2009, requires that all authorized users of DON information systems and networks receive initial IA training. In addition, users should complete annual IA refresher training which should be noted on the SAAR-N in accordance with Navy Telecommunications Directive 10-11. To determine whether the SAAR-N forms were appropriately completed and approved, we verified that the IAM signed the forms and that IA training was completed within a year of the IAM's signature. To determine whether the DD Form 2842 was appropriately completed and approved, we verified that the user and registration official signed and dated the form, and confirmed that the registration official witnessed the user's signature. We performed control tests of the SAAR-N forms and DD Forms 2842.[15]

~~(FOUO)~~ DoDIG (b)(7)(E) System Access Forms Were Not Appropriately Completed or Approved

~~(FOUO)~~ The DoDIG (b)(7)(E) IAM did not complete and approve user network access forms before providing users with SIPRNET access. We requested SAAR-N forms and DD Forms 2842 for a sample of 32 DoDIG (b)(7)(E) personnel. The IAM could only provide 28 SAAR-Ns and 21 DD Forms 2842 and could not explain why the 4 SAAR-N forms and 5 DD Forms 2842 were missing. For the other 6 missing DD Forms 2842 requested, the personnel had not been issued SIPRNET tokens; therefore, the form was not required.

~~(FOUO)~~ We reviewed the 28 SAAR-N forms and determined that the IAM did not sign 1 form. The other 27 forms were signed; however, the signature block was dated the day that the forms were provided to the audit team. In addition, 2 of the forms did not have IA training noted on the form, and 11 forms indicated that IA training was not completed within a year of the IAM's signature. We reviewed the 21 DD Forms 2842 and determined that 15 forms were signed; however, the signature block was dated the day that the forms were provided to the audit team. When asked about witnessing the forms, the IAM stated that she did not witness the users sign them.

[15] (U) We used the control test table developed by Quantitative Methods Division and published in the Council of the Inspectors General on Integrity and Efficiency, "Journal of Public Inquiry," 2012-2013 when performing the control tests.

(~~FOUO~~) This occurred because [redacted] had not established policies and procedures to verify that the required forms for system access were appropriately completed and approved before providing users SIPRNET access. In addition, the [redacted] IAM stated that this occurred because the [redacted] IAM was responsible for approximately 3,000 users and did not complete, approve, and witness the forms as they were received. However, the [redacted] IAM did not adequately perform the duties assigned in the IAM's position description for authorizing all users SIPRNET access forms before granting them a SIPRNET account. The Commander, [redacted], and the Commander, [redacted] should coordinate and establish policies and procedures to verify that the IAM signs required documentation before providing access to the SIPRNET; and establish policies and procedures to review and verify that the registration official signs required documentation before providing users their SIPRNET tokens.

(~~FOUO~~) [redacted] System Access Forms Were Not Appropriately Completed or Approved

(~~FOUO~~) [redacted] did not accurately complete two SAAR-N forms and a DD Form 2842. We requested and received SAAR-N forms and DD Forms 2842 for a sample of 41 [redacted] personnel. We reviewed the 41 SAAR-N forms and determined that 1 form did not document IA training on the form and another form indicated that IA training was not completed within a year of IAM signature, and therefore the control test failed. In addition, we reviewed the 41 DD Forms 2842 and determined that the registration official did not sign or witness the user's signature for 1 form, and therefore the control test failed.

(~~FOUO~~) This occurred because [redacted] had not established procedures to verify that the required forms for system access were appropriately completed before providing users SIPRNET access. On May 1, 2014, [redacted] established a procedure for the [redacted] Security Department to review and verify all SAAR-N forms. [redacted] should implement procedures to review and verify that all DD Forms 2842 are completed before users gain access to the SIPRNET.

~~(FOUO)~~ Security Training Records Were Incomplete

~~(FOUO)~~ [redacted] did not maintain evidence of security training. DoDM 5200.01, volume 3, requires DoD Components to maintain records of employee security training. Specific training required for access to classified information include:

- ~~(FOUO)~~ initial orientation training on security policies as required by DoDM 5200.01, volume 3,
- ~~(FOUO)~~ annual refresher training on security policies, principles, and procedures as required by DoDM 5200.01, volume 3, and
- ~~(FOUO)~~ North Atlantic Treaty Organization (NATO) briefings that discuss the responsibilities for protecting NATO information and a written acknowledgement of the individual's receipt of the briefing, as required by DoDM 5200.01, volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012.

~~(FOUO)~~ [redacted] Training Records Were Incomplete

~~(FOUO)~~ [redacted] did not maintain evidence that personnel completed classified information access training. We requested evidence for completed initial orientation security training, annual security refresher training, and NATO briefings for a sample of 32 personnel. The [redacted] provided evidence that 16 personnel completed the initial orientation security training, but was unable to provide evidence that personnel completed the annual security refresher training and the NATO briefings.

~~(FOUO)~~ [redacted] did not have a process in place to ensure that personnel completed training and that evidence of completion is recorded before granting SIPRNET access. The [redacted] stated that [redacted] provides annual security refresher training and NATO briefings; however, he was not aware that the command needed to maintain evidence of security training completion. [redacted] should complete required security trainings and implement a mechanism to identify individuals who have completed the required training.

~~(FOUO)~~ DoDIG (b)(7)(E) Training Records Were Incomplete

~~(FOUO)~~ DoDIG (b)(7)(E) did not maintain evidence that personnel completed classified information access training. We requested evidence for completed initial orientation security training, annual security refresher training, and NATO briefings for a sample of 41 personnel. DoDIG (b)(7)(E) provided evidence of initial orientation security training for 39 personnel, annual security training for 31 personnel, and NATO briefings for all 41 personnel.

~~(FOUO)~~ For the two personnel we did not receive evidence of initial orientation security training; DoDIG (b)(7)(E) was unsure why one person did not receive initial orientation security training and the Security Officer stated that the other person was a reservist who was rarely at the command and the security staff overlooked the requirement. In addition, DoDIG (b)(7)(E) did not have evidence of annual security training for six personnel because they were not due for annual security training; however, four personnel were missing annual security refresher training because the command was changing how it tracked annual security training, and the new automated tracking system did not record the data correctly.

~~(FOUO)~~ We reviewed the training records provided by DoDIG (b)(7)(E) and determined that 2 of 41 personnel did not have NATO briefings signed by the presenter. This occurred because the presenter signed the NATO briefings at the end of the presentation and two of the training forms were overlooked. Also, DoDIG (b)(7)(E) did not have policies and procedures to track completion of the required security training before granting SIPRNET access. DoDIG (b)(7)(E) should complete required security trainings and implement a procedure for identifying and retaining records of individuals who completed the required training.

~~(FOUO)~~ DoDIG (b)(7)(E)

~~(FOUO)~~ DoDIG (b)(7)(E)

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

~~(S)~~ NAVY (b)(1), Sec 1.4(g) [redacted]

(S) NAVY: (b)(1), Sec 1.4(g) [redacted]

(U) Recommendations, Management Comments, and Our Response

(U) Renumbered Recommendations

(U) We renumbered draft report Recommendation A.2 as A.3. We renumbered draft report Recommendation A.3 as A.2.

(U) A.1. We recommend that the Under Secretary of Defense for Intelligence; Commander, U.S. Cyber Command; and Department of Defense Chief Information Officer, coordinate to review and issue clarifying guidance for the Office of the Secretary of Defense Memorandum "Insider Threat Mitigation," July 12, 2013, instructing DoD Components on the proper procedures for DoDIG (b)(7)(E) [redacted]

(U) Under Secretary of Defense for Intelligence Comments

(~~FOUO~~) The Director for Defense Intelligence (Intelligence & Security), responding on behalf of the Under Secretary of Defense for Intelligence, neither agreed nor disagreed, and stated that since the memorandum was dispatched, Commander, U.S. Cyber Command, issued Task Order 13-0651, "Insider Threat Mitigation Amplifying Direction," July 31, 2013, and Task Order 14-0185, "Insider Threat Initiative," July 17, 2014, that provide explicit guidance to DoD Components regarding DoDIG: (b)(7)(E) [redacted] According to the Director, collaboration with DoD CIO staff confirmed that the two task orders capture requirements to DoDIG: (b)(7)(E) [redacted] The Office of the Under Secretary of Defense for Intelligence acknowledged the DoD OIG comment but requested that the draft report recommendation be withdrawn due to U.S. Cyber Command clarifying guidance.

(U) Our Response

(~~S~~) NAVY (b)(1), Sec 1.4(g) [redacted]

(U) Commander, U.S. Cyber Command Comments

(~~FOUO~~) The Director of Operations, responding on behalf of the Commander, U.S. Cyber Command, neither agreed nor disagreed, and stated that U.S. Cyber Command Task Order 14-0185, "Insider Threat Initiative," July 17, 2014, applies to SIPRNET and provides technical and procedural direction DoDIG: (b)(7)(E) [redacted]

(U) Our Response

(~~S~~) NAVY (b)(1), Sec 1.4(g) [redacted]

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

(U) Department of Defense Chief Information Officer Comments

(U) We received the DoD CIO comments on the draft report too late to include them in the final report. Therefore, if the DoD CIO does not submit additional comments, we will consider those comments as the management response to the final report.

~~(S)~~ **A.2.** NAVY: (b)(1), Sec. 1.4(g) [redacted]

(U) Commander, U.S. Cyber Command Comments

~~(FOUO)~~ The Director of Operations, responding on behalf of the Commander, U.S. Cyber Command, neither agreed nor disagreed, and stated that U.S. Cyber Command will update all applicable orders, including Communications Tasking Order 10-133, to direct DoD Components to DoDIG: (b)(7)(E) [redacted]

(U) Our Response

(U) Comments from the Director addressed all of the specifics of the recommendation. No further comments are required.

(U) A.3. We recommend that the Deputy Under Secretary of the Navy, Policy, update Department of Navy policy to implement at least the minimum requirements for performing a risk assessment as required by DoD Manual 5200.01, volume 3.

(U) Deputy Under Secretary of the Navy, Policy Comments

(U) The Deputy Under Secretary of the Navy, Policy, agreed with the recommendation. The Deputy Under Secretary of the Navy, Policy, Senior Director for Security, stated that the Deputy Under Secretary of the Navy, Policy, is updating the Secretary of the Navy Manual 5510.36, "Department of the Navy Information Security Program," June 2006. The expected timeline for completion of the draft is the end of FY 2015.

(U) Our Response

(U) Comments from the Senior Director addressed all of the specifics of the recommendation. No further comments are required.

(U) A.4. We recommend that the Department of the Navy Chief Information Officer and Department of the Navy Deputy Chief Information Officer (Navy), coordinate to implement requirements from DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, including all links, references, and attachments, DoDIG: (b)(7)(E) [redacted]

(U) Department of the Navy Chief Information Officer Comments

~~(FOUO)~~ The Principal Deputy CIO, responding on behalf of the Department of the Navy CIO, agreed with the recommendation. The Principal Deputy CIO stated that the DON CIO has already begun coordinating the Department's transition to the revised DoD Cybersecurity and Risk Management Framework instructions, including DoD Instruction 8500.01 "Cybersecurity," March 14, 2014. The DON CIO issued a memorandum, "Implementation of the DoD Risk Management Framework for Information Technology (IT)," on May 20, 2014, providing guidance to the Navy and Marine Corps to transition to the DoD Risk Management Framework. In addition, the DON CIO is working with the DON Deputy CIO (Navy) to develop the Navy's Risk Management Framework implementation plan.

(U) Our Response

(U) Comments from the Principal Deputy CIO addressed all of the specifics of the recommendation. No further comments are required.

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ The Assistant Deputy Chief of Naval Operations, Information Dominance, responding on behalf of the DDCIO(N), neither agreed nor disagreed, and stated that the DDCIO(N) continues to coordinate with the DON CIO, U.S. Fleet Cyber Command/U.S. Tenth Fleet, and applicable Echelon II commands on the transition to the revised DoD Cybersecurity and Risk Management Framework to ensure Navy implements DoD Instruction 8500.01 and DoD Instruction 8510.01 requirements, including all links, references, attachments, and DoDIG (b)(7)(E) [redacted]. In addition, the DDCIO(N) hosted a Risk Management Framework implementation working group on October 21-23, 2014 to review the Navy's Risk Management Framework transition plan.

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

(U) Deputy Under Secretary of the Navy, Policy Comments

(U) Although not required to comment, the Deputy Under Secretary of the Navy, Policy, suggested including the Deputy Under Secretary of the Navy, Policy, in the coordination for recommendation A.4.

(U) Our Response

(U) We fully support coordination between the Navy Components; however, our recommendation was directed to the parties responsible for implementing Navy policy. Therefore, we did not change the recommendation to include coordination with the Deputy Under Secretary of the Navy, Policy.

(U) A.5. We recommend that the Department of the Navy Deputy Chief Information Officer (Navy):

a. **~~(FOUO)~~ Review the deficiencies identified, have a thorough review of the Navy Marine Corps Intranet Secret Internet Protocol Router Network security controls performed at each command, and apply corrective actions as necessary.**

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ The Assistant Deputy Chief of Naval Operations, Information Dominance, responding on behalf of the DDCIO(N), neither agreed nor disagreed, and stated that the DDCIO(N) has directed U.S. Fleet Cyber Command/U.S. Tenth Fleet ODAA to review the NMCI SIPRNET security controls enterprise-wide. The review will consist of the following stakeholders: Site/Command IAM, Naval Enterprise Networks, Program Management Office, U.S. Fleet Cyber Command/U.S. Tenth Fleet Network Operations, and the ODAA, who will coordinate to ensure the results and corrective actions are used to determine the impact of the DoDIG (b)(7)(E) [redacted]. The coordination with stakeholders will take place no later than November 15, 2014.

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

b. **~~(FOUO)~~ Implement the requirements for performing a risk assessment in accordance with updated Department of Navy policy and DoD 5200.01, volume 3.**

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ The Assistant Deputy Chief of Naval Operations, Information Dominance, responding on behalf of the DDCIO(N), neither agreed nor disagreed, and stated that the DDCIO(N) has issued an DoDIG (b)(7)(E) [redacted] The Site/Command IAM and Naval Enterprise Networks, Program

~~(FOUO)~~ Management Office will work to implement the requirements in accordance with DoD 5200.01, Volume 3, and transmit information to the ODAA, who will use the results to determine the impact to the DoDIG (b)(7)(E). The estimated timeline for this action is no later than November 15, 2014. A risk assessment is part of the physical security control assessment required for system accreditation under DoD Instruction 8510.01 and forthcoming Secretary of the Navy and Chief of Naval Operations guidance. Chief of Naval Operations Instruction 5239.1D is expected to be published by January 31, 2015.

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

~~(FOUO)~~ A.6. We recommend that the DoDIG (b)(7)(E); coordinate and review the actions of the Information Assurance Manager for the DoDIG (b)(7)(E) regarding the deficiencies identified in this report. Based on that review, the DoDIG (b)(7)(E), should take appropriate management action, including holding the Information Assurance Manager accountable.

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ The Assistant Deputy Chief of Naval Operations, Information Dominance, responding on behalf of DoDIG (b)(7)(E) neither agreed nor disagreed, and stated that the supervision and accountability of DoDIG (b)(7)(E) Information Assurance Officer resides with the DoDIG (b)(7)(E) Commanding Officer. The DoDIG (b)(7)(E) Information Assurance Officer no longer provides Information Assurance services to DoDIG (b)(7)(E). The DoDIG (b)(7)(E) provides services for all SIPRNET account requests, SAAR-N compliance, and token requests.

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance did not address the specifics of the recommendation. The DoDIG (b)(7)(E) [redacted] did not comment on the review of the IAM actions and the corresponding management actions taken for holding the IAM accountable. Therefore, we request the DoDIG (b)(7)(E) [redacted] provide comments in response to the final report.

(U) A.7. We recommend that DoDIG (b)(7)(E) [redacted] **coordinate and establish:**

a. ~~**(FOUO)**~~ DoDIG (b)(7)(E) [redacted]

b. ~~**(FOUO)**~~ DoDIG (b)(7)(E) [redacted]

c. ~~**(FOUO)**~~ DoDIG (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ The Assistant Deputy Chief of Naval Operations, Information Dominance, responding on behalf of the DoDIG (b)(7)(E) [redacted] neither agreed nor disagreed, and stated that DoDIG (b)(7)(E) [redacted] no longer

~~(FOUO)~~ provides Information Assurance services to DoDIG (b)(7)(E). DoDIG (b)(7)(E)

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

(U) A.8. We recommend that DoDIG (b)(7)(E)

a. **(U) Review the alignment of the Information Assurance Manager function, determine if realignment is necessary for effective supervision, and establish policy that assigns supervisory responsibility.**

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ The Assistant Deputy Chief of Naval Operations, Information Dominance, responding on behalf of the DoDIG (b)(7)(E) neither agreed nor disagreed, and stated that DoDIG (b)(7)(E) no longer receives IA services from DoDIG (b)(7)(E). Supervision and accountability of DoDIG (b)(7)(E) Information Assurance Officer resides with the DoDIG (b)(7)(E) Commanding Officer.

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. As discussed in the comments and response to Recommendation A.7, the DoDIG: (b)(7)(E) has supervisory responsibility for the DoDIG: (b)(7)(E) Information Assurance Officer. A Memorandum of Agreement between the DoDIG: (b)(7)(E) discussing the supervision and responsibilities for the DoDIG: (b)(7)(E) Information Assurance Officer, was provided. We reviewed the Memorandum of Agreement and determined that it meets the intent of the recommendation. No further comments are required.

b. **(U) Establish and implement performance standards and standard operating procedures for the Information Assurance Manager function, and monitor and evaluate the Information Assurance Managers' performance.**

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ The Assistant Deputy Chief of Naval Operations, Information Dominance, responding on behalf of the DoDIG: (b)(7)(E) neither agreed nor disagreed, and stated that the DDCIO(N) will request that Chief of Naval Operations direct DoDIG: (b)(7)(E) personnel to provide documentation that they have implemented performance standards and standard operating procedures for the IAM no later than November 30, 2014.

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

(U) A.9. We recommend that DoDIG: (b)(7)(E) [redacted]

a. **~~(FOUO)~~** DoDIG: (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ The Assistant Deputy Chief of Naval Operations, Information Dominance, responding on behalf of the DoDIG: (b)(7)(E) [redacted], neither agreed nor disagreed, and stated that the DoDIG: (b)(7)(E) [redacted] IAM conducts the DoDIG: (b)(7)(E) [redacted]. The Deputy Chief of Naval Operations (N2/N6) will direct U.S. Fleet Forces Command/Tenth Fleet to provide documentation of DoDIG: (b)(7)(E) [redacted] within the past 6 months.

(U) Our Response

~~(FOUO)~~ Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance partially addressed the recommendation. We request that DoDIG: (b)(7)(E) [redacted] provide comments to the final report that explicitly state whether a DoDIG: (b)(7)(E) [redacted] has been performed within the past 6 months or if one has not been performed, a DoDIG: (b)(7)(E) [redacted] should be performed immediately.

b. **~~(FOUO)~~** DoDIG: (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ The Assistant Deputy Chief of Naval Operations, Information Dominance, responding on behalf of the DoDIG (b)(7)(E) [redacted], neither agreed nor disagreed, and stated that the DoDIG (b)(7)(E) [redacted]

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

c. **~~(FOUO)~~ Complete required security trainings and develop and implement a mechanism for identifying individuals who complete required security training.**

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ The Assistant Deputy Chief of Naval Operations, Information Dominance, responding on behalf of the DoDIG (b)(7)(E) [redacted], neither agreed nor disagreed, and stated that initial security training is conducted when military, civilian, and contractor personnel report onboard and is documented in security files. Annual security refresher training is conducted and documented as required by current instructions.

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance partially addressed the recommendation. We request that DoDIG (b)(7)(E) [redacted] officials provide comments to the final report that describe the mechanism that will be used to identify individuals who complete the required security training.

~~(S)~~ A.10. NAVY (b)(1), Sec 1.4(g) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(S)~~ NAVY (b)(1), Sec 1.4(g) [redacted]

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

(U) A.11. We recommend that DoDIG (b)(7)(E) [redacted]

a. ~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ The Assistant Deputy Chief of Naval Operations, Information Dominance, responding on behalf of the DoDIG (b)(7)(E) [redacted] neither agreed nor disagreed, and stated that DoDIG (b)(7)(E) [redacted] has corrected deficiencies with its secure room in a manner compliant with DoDM 5200.01, Volume 3, ensuring continuous monitoring during working hours when the secure door is unlocked.

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

b. ~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

(U) Our Response

~~(FOUO)~~ Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance partially addressed the recommendation. DoDIG (b)(7)(E) [redacted]

c. ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

(U) Our Response

~~(FOUO)~~ Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

d. ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

(U) Our Response

~~(FOUO)~~ Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance partially addressed the recommendation. We request that DoDIG (b)(7)(E) [redacted] provide additional comments that describe the procedures for performing risk assessments in response to the final report.

e. **~~(FOUO)~~ Complete required security training and develop and implement a mechanism to identify individuals who complete required security training.**

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ The Assistant Deputy Chief of Naval Operations, Information Dominance, responding on behalf of the DoDIG (b)(7)(E) [redacted] neither agreed nor disagreed, and stated that DoDIG (b)(7)(E) [redacted] will conduct a physical security training audit, identify deficiencies, and conduct required training no later than November 15, 2014. Proof of training completion will be reported to DoDIG (b)(7)(E) [redacted] The Chief of Naval Operations (N2/N6) will request that Commander, Navy Reserve Forces Command provide documentation of the DoDIG (b)(7)(E) [redacted] physical security training audit no later than November 30, 2014.

(U) Our Response

~~(FOUO)~~ Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance partially addressed the recommendation. We request that DoDIG (b)(7)(E) [redacted] officials provide additional comments that address all security training not just physical security training. Also, provide comments that describe the mechanism, which should be of a recurring nature, that will be used to identify individuals who complete the required security training in response to the final report.

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ Although not required to comment, the Assistant Deputy Chief of Naval Operations, Information Dominance, responding on behalf of the DoDIG (b)(7)(E) [redacted], stated that DoDIG (b)(7)(E) [redacted] requires DoDIG (b)(7)(E) [redacted]

(U) Our Response

(U) Although the comments from the Assistant Deputy Chief of Naval Operations, Information Dominance do not directly address any recommendation, we agree with DoDIG (b)(7)(E) [redacted] in accordance with DODI 8500.01, "Cybersecurity, " March 14, 2014.

(U) Finding B

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

- ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]
- ~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted] [redacted] [redacted]
- ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]
- ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

(U) [16] Vulnerabilities are also known as security weaknesses.

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

~~(FOUO)~~ During the audit, DoD issued updated policy for the certification and accreditation of systems, DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014. According to DoDI 8510.01, DoD Components should transition to the updated policy requirements when reaccreditation is necessary. DoDIG (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

(U) DoDIG: (b)(7)(E) [redacted]

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

(S) NAVY: (b)(1), Sec. 1.4(g) [redacted]

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

(U) [17] The Readiness Inspection results were presented by DoDIG: (b)(7)(E) [redacted]

(U) [18] The Enterprise POA&M lists DoDIG: (b)(7)(E) [redacted].

(U) [19] The Validation Plan and Procedures and Risk Assessment Reports are internally generated documents that identify vulnerabilities and their associated severity CAT.

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

- ~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

- ~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

(U) DoDIG: (b)(7)(E) [redacted]

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

(U) [20] A cross-domain solution is an information assurance solution that provides the ability to access or transfer data between two or more differing security domains, and can be authorized for no more than one year from the date of approval. Domains include a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

(~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

(~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

(~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

(~~FOUO~~) *Table 1.* DoDIG: (b)(7)(E) [redacted]

DoDIG: (b)(7)(E) [redacted]

(~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted] [redacted] [redacted]

(U) [21] A network topology depicts the security posture of the network enclave that will be connecting to the DISN.

~~(FOUO)~~ *Table 2.* DoDIG (b)(7)(E) [redacted]

DoDIG (b)(7)(E) [redacted]

(U) * Time lapsed before DISA approval refers to the time between when the configuration change was implemented and when DISA issued the Authority to Connect.
(U) ** Intrusion detection system

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

(U) [22] Enclaves are a collection of information systems connected by one or more internal networks under the control of a single authority and security policy.

(~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

(~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

(~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

(U) According to DISA, "Network Infrastructure Technology Overview," version 8, release 5, April 27, 2012, enabled tunnels should be identified on the network topology. In addition, according to the DISN Connection Process Guide, the network topology is required to show the accreditation boundaries,[23] identify cross-domain solution, and identify any connections to other networks to include the name of the organization that owns the enclave, the connection type, internet protocol addresses for all devices within the enclave, and the organization type.

(~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

(U) [23] Accreditation boundary refers to the physical or logical boundary that is defined for a system, domain, or enclave. The system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected.

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

(U) Recommendations, Management Comments, and Our Response

~~(FOUO)~~ **B.1.** DoDIG: (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

~~(FOUO)~~ B.2. DoDIG (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

(U) B.3. We recommend that the Director, Navy Operational Designated Accrediting Authority:

a. **~~(FOUO)~~** DoDIG (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

b. ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

(~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

c. (~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

(~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

d. (~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance did not address the specifics of the recommendation. However, as discussed in the comments to Recommendation B.2, DoDIG (b)(7)(E) [redacted], and therefore no further comments are required.

e. ~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted]

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

(~~FOUO~~) B.4. DoDIG: (b)(7)(E) [redacted]

- **(~~FOUO~~)** DoDIG: (b)(7)(E) [redacted]
- **(~~FOUO~~)** DoDIG: (b)(7)(E) [redacted]

(U) Assistant Deputy Chief of Naval Operations, Information Dominance Comments

(~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

(U) Our Response

(U) Comments from the Assistant Deputy Chief of Naval Operations, Information Dominance addressed all of the specifics of the recommendation. No further comments are required.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from April 2013 through September 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) We performed the audit to determine whether the Navy was effectively protecting SIPRNET access points. DoDIG (b)(7)(E) [redacted] The commands chosen represented various types of access points, Sensitive Compartmented Information Facility, Open Secret Storage, and Secure Room as designated by the U.S. Navy. DoDIG (b)(7)(E) [redacted]

~~(FOUO)~~ DoDIG (b)(7)(E) [redacted] For more information on certification and accreditation activities, see Appendix B.

(U) During our review, we interviewed DoD and Navy component personnel. We interviewed personnel at the Under Secretary of Defense for Intelligence, DoD CIO, and U.S. Cyber Command concerning the write privilege criteria. We interviewed personnel at DDCIO(N) to discuss SIPRNET access points, and open NMCI vulnerabilities. At the DoDIG (b)(7)(E) [redacted] we interviewed personnel; obtained, reviewed, and analyzed policies; obtained, reviewed,

(U) and analyzed network access and privilege processes; and obtained, reviewed, and analyzed network settings. At DoDIG: (b)(7)(E) [redacted], we interviewed personnel; obtained, reviewed, and analyzed physical security, logical security, user authentication, personnel access, classified information protection, visitor access, and classified information technology disposal policies and procedures; and observed physical security for SIPRNET access points.

(U) In addition, we performed control tests for the SAAR-N forms, DD Forms 2842, and security training forms. DoDIG: (b)(7)(E) [redacted] The following decision rules applied for our control tests: if there were no errors in the sample, then the control passes, and if there were one or more errors, then the control fails. We used the control test table developed by Quantitative Methods Division and published in the Council of the Inspectors General on Integrity and Efficiency, "Journal of Public Inquiry," 2012-2013 when performing the control tests.

(U) DoDIG: (b)(7)(E) [redacted]

(U) Use of Computer-Processed Data

~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

(~~FOUO~~) DoDIG (b)(7)(E) [redacted]

(~~FOUO~~) DoDIG (b)(7)(E) [redacted]

(~~FOUO~~) DoDIG (b)(7)(E) [redacted]

(U) Use of Technical Assistance

(U) We obtained support from the DoD Office of the Inspector General Quantitative Methods Division in developing a statistical sample for review. We obtained support from the DoD Office of the Inspector General Information Systems Directorate for defining SIPRNET access points.

(U) Prior Coverage

(U) During the last 5 years, the Naval Audit Service issued one report discussing security guidance for certification and accreditation.

(U) Navy Audit Service

(U) N2012-0070, "Navy Compliance with Department of Defense Information Assurance Certification and Accreditation Process," September 28, 2012

(U) Appendix B

(U) DoD Information Assurance Certification and Accreditation Process

(U) The DIACAP establishes a process to certify and accredit DoD information systems based on the implementation of IA controls. DIACAP applies to all DoD-owned and controlled information systems and consists of five activities:

- (U) Activity 1: Initiate Certification and Accreditation — includes registering the system with the appropriate DoD Component, assigning IA controls to the information system, and initiating the DIACAP Implementation Plan. Each assigned control is implemented according to the applicable implementation guidelines provided in the DIACAP.
- (U) Activity 2: Implement and Validate IA Controls — includes executing the DIACAP Implementation Plan, conducting validation activities, preparing the IT Security POA&M, and compiling validation results in the DIACAP Scorecard. The status of each assigned IA control is indicated on the DIACAP Scorecard as compliant, noncompliant, or not applicable.
- (U) Activity 3: Make Certification Determination and Accreditation Decision — includes determining whether to certify and accredit a DoD information system. Each information system has a certifying authority, who bases the certification decision on IA validation results, and a designated accrediting authority, who bases the accreditation decision on a balance of mission or business need and protection of the information being processed.

- (U) Activity 4: Maintain Authorization — involves the sustainment of acceptable IA posture. The IA controls should be reviewed annually to confirm the effectiveness of the assigned IA controls or to recommend changes to the accreditation status. A designated accrediting authority may downgrade or revoke an accreditation decision at any time if risk conditions or concerns develop from the reviews. The results of an annual review or a major change in information assurance posture at any time may indicate the need for recertification and reaccreditation.
- (U) Activity 5: Decommissioning — focuses on removing DoD information system from operation.

(U) Appendix C

(U) Information Assurance Controls

(U) According to DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, IA controls are an objective condition of the integrity, availability, or confidentiality of the information system achieved through the application of specific safeguards or through the regulation of specific activities. There are eight broad IA control subject areas:

- (U) Security Design and Configuration, abbreviated DC;
- (U) Identification and Authentication, abbreviated IA;
- (U) Enclave and Computing Environment, abbreviated EC;
- (U) Enclave Boundary Defense, abbreviated EB;
- (U) Physical and Environmental, abbreviated PE;
- (U) Personnel, abbreviated PR;
- (U) Continuity, abbreviated CO; and
- (U) Vulnerability and Incident Management, abbreviated VI.

(U) Each IA control is assigned a control number that designates the control's subject area and name. The control numbers consist of four letters, a dash, and a number. The first two letters designate the subject area and the second two letters designate the control name. The number represents a level of robustness of the IA control in ascending order, with one being the least robust and a three being the most robust. See Table 1 for a description of the IA controls discussed in our report including the control number and the corresponding subject areas and control names.

~~(FOUO)~~ Table C.1. Information Assurance Controls

~~(FOUO)~~ Control Number	Subject Area	Control Name
DoDIG (b)(7)(E) [redacted]	[redacted]	[redacted]

(U) Appendix D

~~(S)~~ NAVY: (b)(1), Sec. 1.4(g) [redacted]

NAVY: (b)(1), Sec. 1.4(g) [redacted]

(U) * DoDIG: (b)(7)(E) [redacted]

[1] (U) CAT I vulnerabilities are the most critical and are required to be corrected before an ATO is granted. CAT II vulnerabilities can lead to unauthorized system access or activity, and are required to be corrected or mitigated within 180 days of granting an ATO. If vulnerabilities are not corrected or mitigated within the specified time frame, the ATO becomes invalid. CAT III vulnerabilities may impact security posture but are not required to be mitigated or corrected in order for an ATO to be granted.

(U) Appendix E

(U) Criteria

(U) We used the following guidance throughout the audit.

(U) National Security Telecommunications and Information Systems Security Committee

(U) National Security Telecommunications and Information Systems Security Instruction 7003, "Protected Distribution Systems," December 13, 1996, outlines the approval authority, standards, and guidance for PDS design, installation, and maintenance.

(U) Office of the Secretary of Defense

(U) Office of the Secretary of Defense Memorandum "Insider Threat Mitigation," July 12, 2013, provides information protection and insider threat mitigation procedures to be implemented by all DoD Components.

(U) Chairman of the Joint Chiefs of Staff

(U) Chairman of the Joints Chiefs of Staff Instruction 6211.02D, "Defense Information Systems Network (DISN) Responsibilities," Jan 24, 2012, establishes policy and responsibilities for the connection of information systems and unified capabilities products to the DISN-provided transport and access to information services transmitted over the DISN.

(U) DoD

(U) DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks.

(U) DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007, establishes a certification and accreditation process to manage the implementation of IA capabilities and services and provide

(U) visibility of accreditation decisions regarding the operation of DoD information systems, including core enterprise services and Web service-based software systems and applications.

(U) DoDI 8510.01, " Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, provides procedural guidance for the reciprocal acceptance of authorization decisions and artifacts within DoD, and between DoD and other Federal agencies, for the authorization and connection of information systems.

(U) DoDM 5200.01, volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, implements policy, assigns responsibilities, and provides procedures for the designation, marking, protection, and dissemination of controlled unclassified information and classified information, including information categorized as collateral, sensitive compartmented information, and Special Access Program.

(U) DoDM 5200.01, volume 3, "DoD Information Security Program: Protection of Classified Information," March 19, 2013, provides guidance for safeguarding, storing, destroying, transmitting, and transporting classified information and also identifies security education and training requirements and processes for handling of security violations and compromise of classified information.

(U) U.S. Cyber Command

~~(FOUO)~~ U.S. Cyber Command Communications Tasking Order 10-133, "Protection of Classified Information on DoD Secret Internet Protocol Router Network (SIPRNet) Change 2," January 4, 2011, DoDIG (b)(7)(E) [redacted]

(U) Navy

(U) Secretary of the Navy Instruction 5239.3B, "Department of the Navy Information Assurance Policy," June 17, 2009, establishes IA policy for the DON consistent with national and DoD policies.

(U) Secretary of the Navy Manual 5510.36, "Department of the Navy Information Security Program," June 2006, establishes uniform policies and procedures for classifying, safeguarding, transmitting, and destroying classified information. In addition, the manual provides guidance on security education and the industrial security program.

(U) DON, "DoD Information Assurance Certification and Accreditation Process (DIACAP) Handbook," version 1, July 15, 2008, details the baseline DON approach to the DIACAP and the procedures necessary to obtain an accreditation decision for DON information systems undergoing the certification and accreditation actions as required under Federal law, DoD and DON regulations and directives.

(U) Navy Telecommunications Directive 10-11, "OPNAV Form 5239-14/System Access Authorization Request Navy (SAAR-N)," October 2011, requires all users accessing Navy IT resources to sign a SAAR-N form and complete DoD Annual IA training.

(U) Defense Information Systems Agency

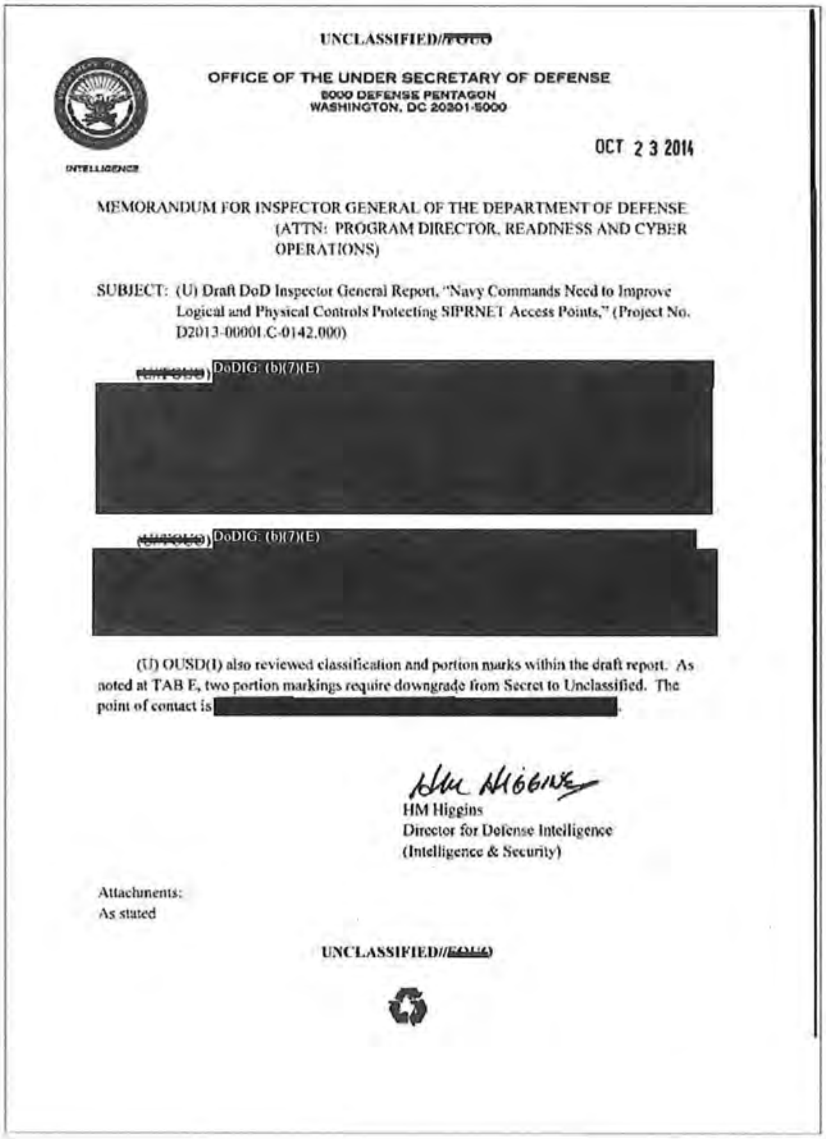
(U) DISA, "Defense Information Systems Network (DISN) Connection Process Guide (CPG)," version 4.2, January 2013, establishes, manages, maintains, and promulgates a partner connection process guide describing steps that must be. followed to request and implement a DISN connection.

(U) DISA, "Network Infrastructure Technology Overview," version 8, release 5, April 27, 2012, provides security considerations at the network level needed for an acceptable level of risk for information as it is transmitted throughout the enclave.

(U) Management Comments

(U) Under Secretary of Defense for Intelligence

Final Report Reference



UNCLASSIFIED//~~FOUO~~

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

INTELLIGENCE

OCT 2 3 2014

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE (ATTN: PROGRAM DIRECTOR, READINESS AND CYBER OPERATIONS)

SUBJECT: (U) Draft DoD Inspector General Report, "Navy Commands Need to Improve Logical and Physical Controls Protecting SIPRNET Access Points," (Project No. D2013-D000I.C-0142.000)

(~~U//FOUO~~) DoDIG: (b)(7)(E) [redacted]

(~~U//FOUO~~) DoDIG: (b)(7)(E) [redacted]

(U) OUSD(I) also reviewed classification and portion marks within the draft report. As noted at TAB F, two portion markings require downgrade from Secret to Unclassified. The point of contact is [redacted].

HM Higgins
HM Higgins
Director for Defense Intelligence
(Intelligence & Security)

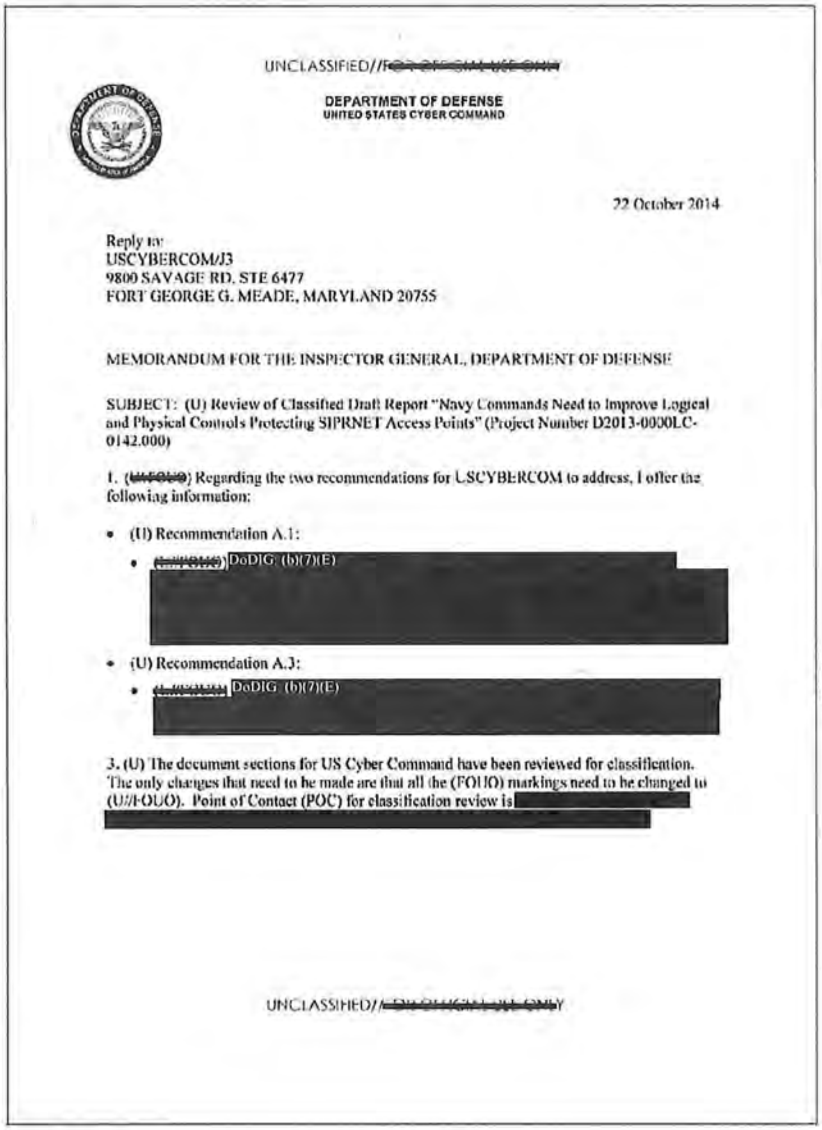
Attachments:
As stated

UNCLASSIFIED//~~FOUO~~

Omitted attachments because of length. Copies provided upon request.

(U) U.S. Cyber Command

Final Report Reference



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND

22 October 2014

Reply to:
USCYBERCOM/J3
9800 SAVAGE RD, STE 6477
FORT GEORGE G. MEADE, MARYLAND 20755

MEMORANDUM FOR THE INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: (U) Review of Classified Draft Report "Navy Commands Need to Improve Logical and Physical Controls Protecting SIPRNET Access Points" (Project Number D2013-0000LC-0142.000)

1. (~~U//FOUO~~) Regarding the two recommendations for USCYBERCOM to address, I offer the following information:

- (U) Recommendation A.1:
    - (~~U//FOUO~~) DoDIG (b)(7)(E) [redacted]
- (U) Recommendation A.3:
    - (~~U//FOUO~~) DoDIG (b)(7)(E) [redacted]

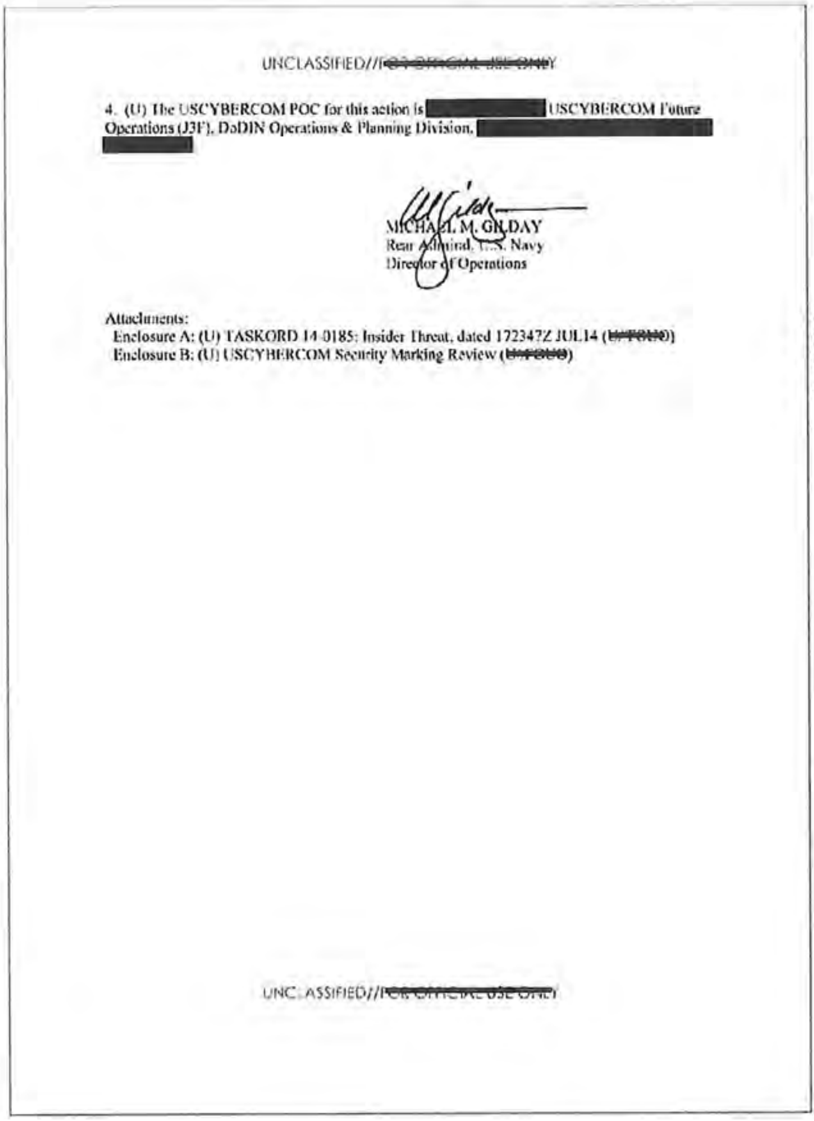
Renumbered as Recommendation A.2.

3. (U) The document sections for US Cyber Command have been reviewed for classification. The only changes that need to be made are that all the (FOUO) markings need to be changed to (U//FOUO). Point of Contact (POC) for classification review is [redacted]

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) U.S. Cyber Command (cont'd)

Final Report Reference



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

4. (U) The USCYBERCOM POC for this action is [redacted] USCYBERCOM Future Operations (J3F), DoDIN Operations & Planning Division, [redacted]

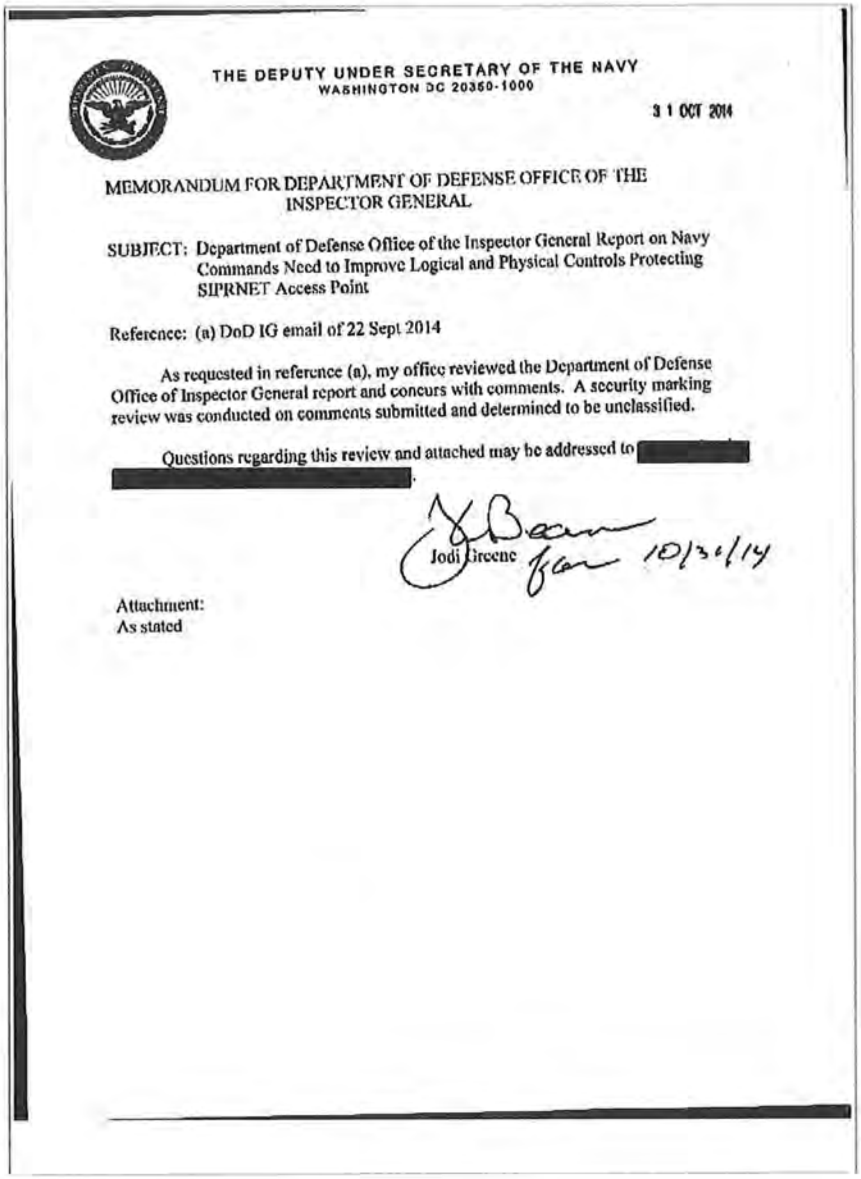
MICHAEL M. GILDAY
Rear Admiral, U.S. Navy
Director of Operations

Attachments:
Enclosure A: (U) TASKORD 14-0185: Insider Threat, dated 172347Z JUL14 (~~U//FOUO~~)
Enclosure B: (U) USCYBERCOM Security Marking Review (~~U//FOUO~~)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Omitted attachments because of length. Copies provided upon request.

(U) Deputy Under Secretary of the Navy



THE DEPUTY UNDER SECRETARY OF THE NAVY
WASHINGTON DC 20350-1000

31 OCT 2014

MEMORANDUM FOR DEPARTMENT OF DEFENSE OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Department of Defense Office of the Inspector General Report on Navy Commands Need to Improve Logical and Physical Controls Protecting SIPRNET Access Point

Reference: (a) DoD IG email of 22 Sept 2014

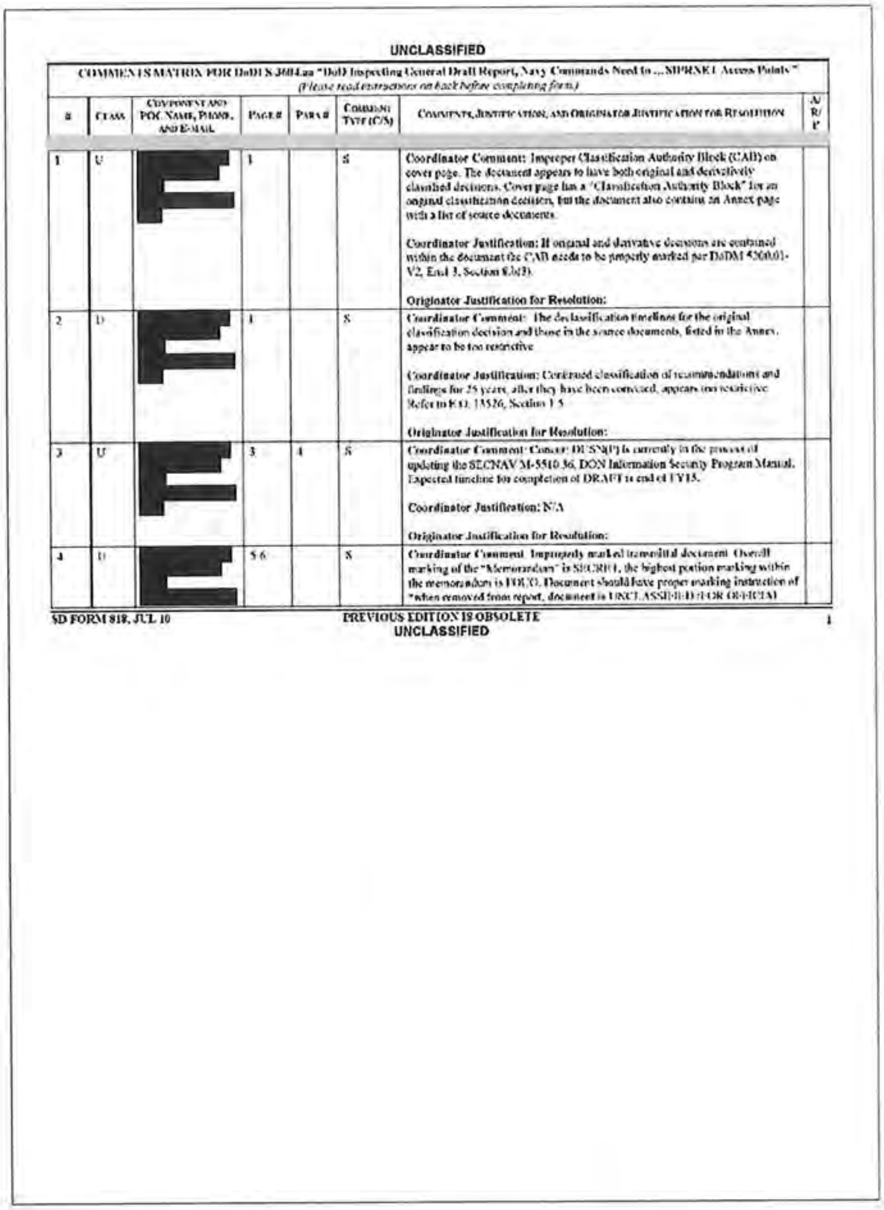
As requested in reference (a), my office reviewed the Department of Defense Office of Inspector General report and concurs with comments. A security marking review was conducted on comments submitted and determined to be unclassified.

Questions regarding this review and attached may be addressed to [redacted].

Jodi Greene for 10/31/14

Attachment:
As stated

(U) Deputy Under Secretary of the Navy (cont'd)



UNCLASSIFIED

COMMENTS MATRIX FOR DoDIG 3004aa "DoD Inspecting General Draft Report, Navy Commands Need to ... SIPRNET Access Points"
(Please read instructions on back before completing form.)

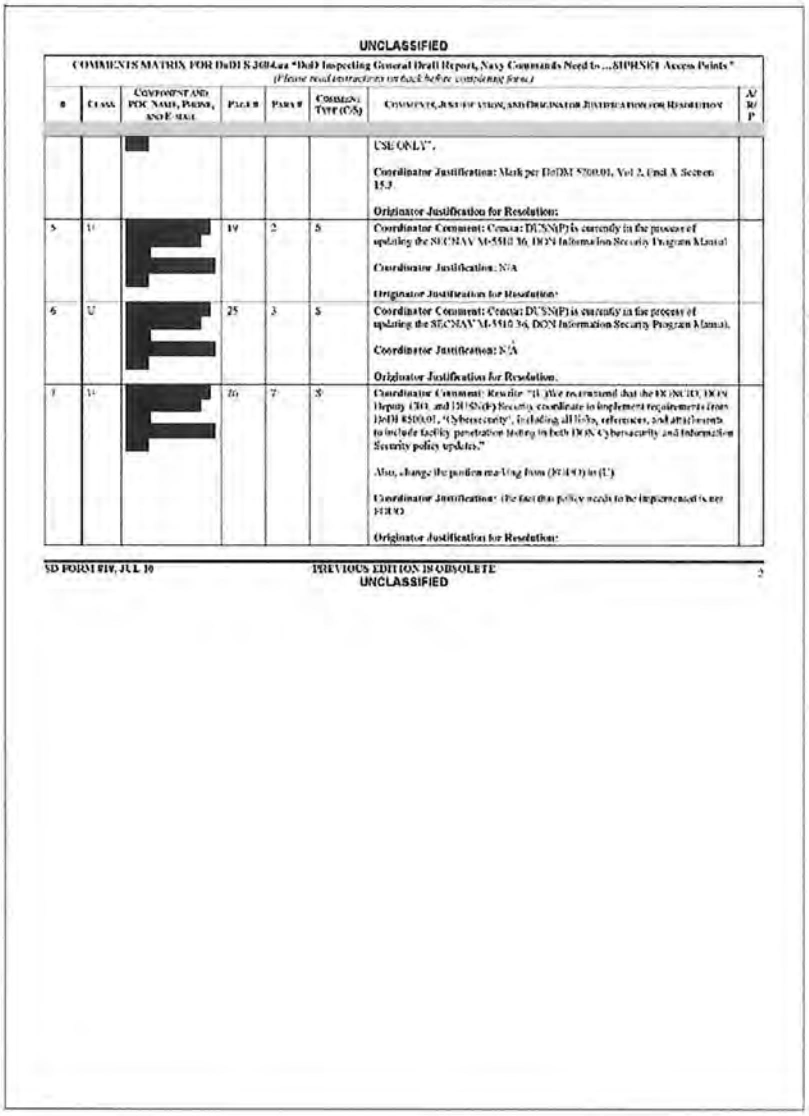
#	Class	Component and POC Name, Phone, and E-Mail	Page #	Para #	Comment Type (C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
1	U	[redacted]	1		S	**Coordinator Comment:** Improper Classification Authority Block (CAB) on cover page. The document appears to have both original and derivatively classified decisions. Cover page has a "Classification Authority Block" for an original classification decision, but the document also contains an Annex page with a list of source documents. **Coordinator Justification:** If original and derivative decisions are contained within the document the CAB needs to be properly marked per DoDM 5200.01-V2, Encl 3, Section 6.b(3). **Originator Justification for Resolution:**	
2	U	[redacted]	1		S	**Coordinator Comment:** The declassification timelines for the original classification decision and those in the source documents, listed in the Annex, appear to be too restrictive **Coordinator Justification:** Continued classification of recommendations and findings for 25 years, after they have been corrected, appears too restrictive. Refer to E.O. 13526, Section 1.5. **Originator Justification for Resolution:**	
3	U	[redacted]	3	4	S	**Coordinator Comment:** Concur. DUSN(P) is currently in the process of updating the SECNAV M-5510.36, DON Information Security Program Manual. Expected timeline for completion of DRAFT is end of FY15. **Coordinator Justification:** N/A **Originator Justification for Resolution:**	
4	U	[redacted]	5-6		S	**Coordinator Comment:** Improperly marked transmittal document. Overall marking of the "Memorandum" is SECRET, the highest portion marking within the memorandum is FOUO. Document should have proper marking instruction of "when removed from report, document is UNCLASSIFIED//FOR OFFICIAL	

SD FORM 818, JUL 10 PREVIOUS EDITION IS OBSOLETE 1

UNCLASSIFIED

(U) Deputy Under Secretary of the Navy (cont'd)

Final Report Reference



UNCLASSIFIED

COMMENTS MATRIX FOR DoDI S 2084.aa "DoD Inspecting General Draft Report, Navy Commands Need to ...SIPRNET Access Points"
(Please read instructions on back before completing form.)

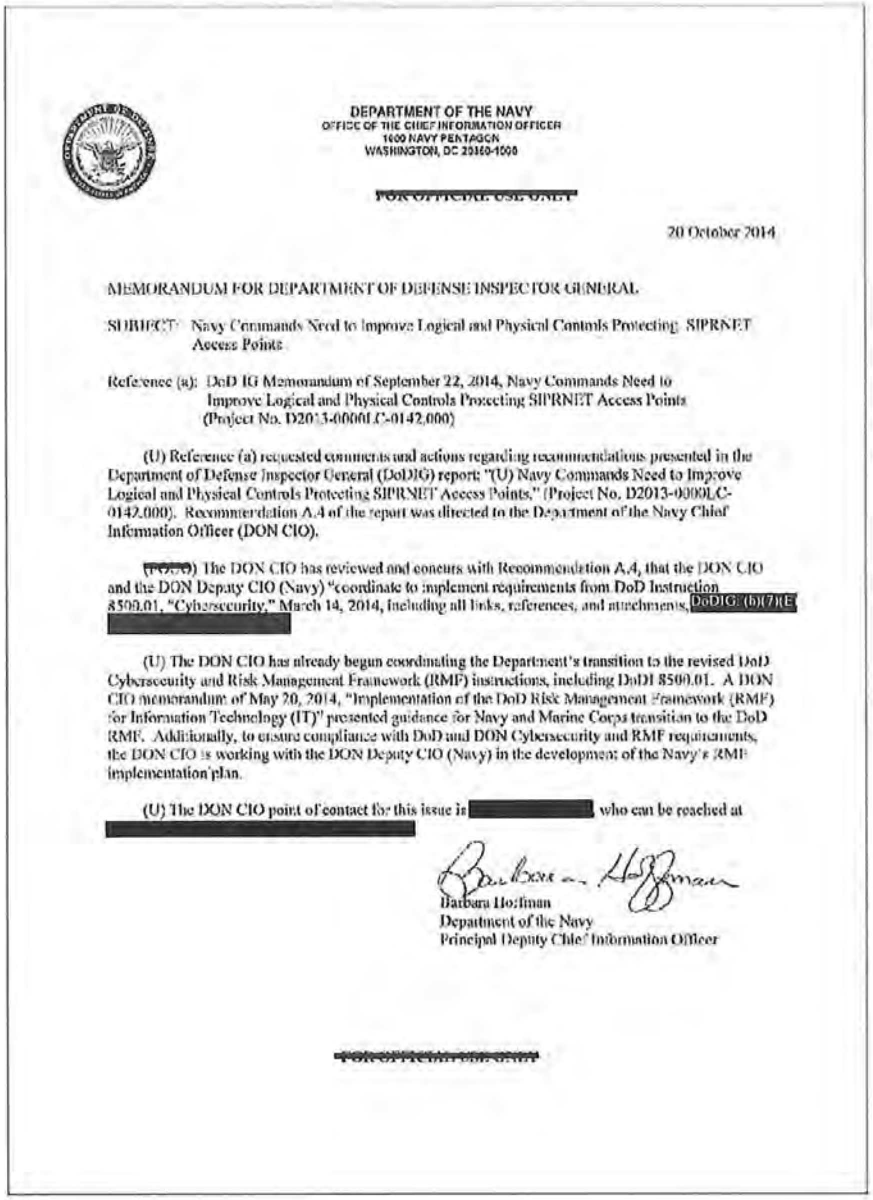
#	Class	Component and POC Name, Phone, and E-mail	Page #	Para #	Comment Type (C/S)	Comments, Justification, and Originator Justification for Resolution	A/R/P
		[redacted]				USE ONLY". **Coordinator Justification:** Mark per DoDM 5200.01, Vol 2, Encl A Section 15.3. **Originator Justification for Resolution:**	
5	U	[redacted]	19	2	S	**Coordinator Comment:** Concur: DUSN(P) is currently in the process of updating the SECNAV M-5510.36, DON Information Security Program Manual **Coordinator Justification:** N/A **Originator Justification for Resolution:**	
6	U	[redacted]	25	3	S	**Coordinator Comment:** Concur: DUSN(P) is currently in the process of updating the SECNAV M-5510.36, DON Information Security Program Manual. **Coordinator Justification:** N/A **Originator Justification for Resolution.**	
7	U	[redacted]	26	7	S	**Coordinator Comment:** Rewrite "(U) We recommend that the DON CIO, DON Deputy CIO, and DUSN(P) Security coordinate to implement requirements from DoDI 8500.01, "Cybersecurity", including all links, references, and attachments to include facility penetration testing in both DON Cybersecurity and Information Security policy updates." Also, change the portion marking from (FOUO) to (U). **Coordinator Justification:** The fact that policy needs to be implemented is not FOUO. **Originator Justification for Resolution:**	

SD FORM 818, JUL 10 PREVIOUS EDITION IS OBSOLETE 2

UNCLASSIFIED

Renumbered as Recommendation A.3.

(U) Department of the Navy Chief Information Officer



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

~~FOR OFFICIAL USE ONLY~~

20 October 2014

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Navy Commands Need to Improve Logical and Physical Controls Protecting SIPRNET Access Points

Reference (a): DoD IG Memorandum of September 22, 2014, Navy Commands Need to Improve Logical and Physical Controls Protecting SIPRNET Access Points (Project No. D2013-0000LC-0142.000)

(U) Reference (a) requested comments and actions regarding recommendations presented in the Department of Defense Inspector General (DoDIG) report: "(U) Navy Commands Need to Improve Logical and Physical Controls Protecting SIPRNET Access Points," (Project No. D2013-0000LC-0142.000). Recommendation A.4 of the report was directed to the Department of the Navy Chief Information Officer (DON CIO).

(~~FOUO~~) The DON CIO has reviewed and concurs with Recommendation A.4, that the DON CIO and the DON Deputy CIO (Navy) "coordinate to implement requirements from DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, including all links, references, and attachments, DoDIG: (b)(7)(E [redacted]

(U) The DON CIO has already begun coordinating the Department's transition to the revised DoD Cybersecurity and Risk Management Framework (RMF) instructions, including DoDI 8500.01. A DON CIO memorandum of May 20, 2014, "Implementation of the DoD Risk Management Framework (RMF) for Information Technology (IT)" presented guidance for Navy and Marine Corps transition to the DoD RMF. Additionally, to ensure compliance with DoD and DON Cybersecurity and RMF requirements, the DON CIO is working with the DON Deputy CIO (Navy) in the development of the Navy's RMF implementation plan.

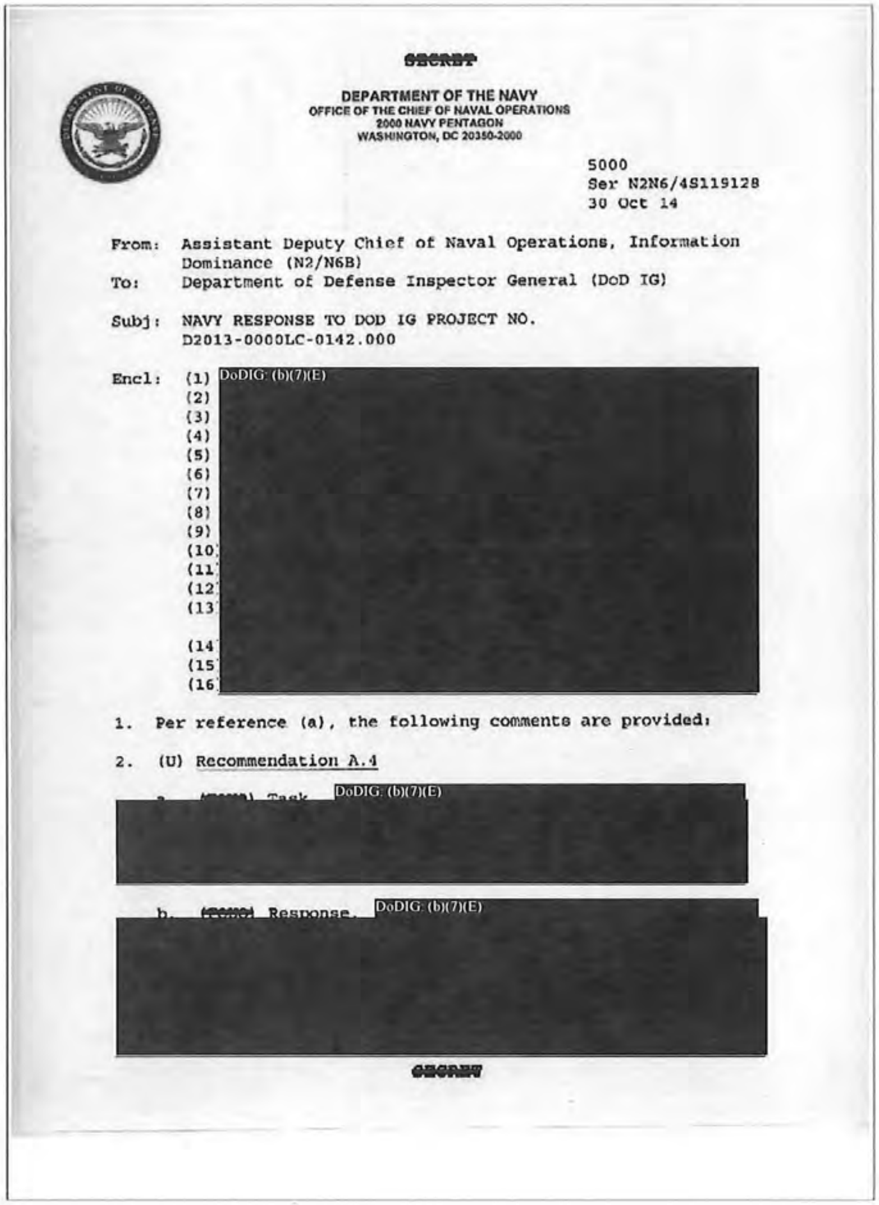
(U) The DON CIO point of contact for this issue is [redacted], who can be reached at [redacted]

Barbara Hoffman

Barbara Hoffman
Department of the Navy
Principal Deputy Chief Information Officer

~~FOR OFFICIAL USE ONLY~~

(U) Assistant Deputy Chief of Naval Operations, Information Dominance



~~SECRET~~

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, DC 20350-2000

5000
Ser N2N6/4S119128
30 Oct 14

From: Assistant Deputy Chief of Naval Operations, Information Dominance (N2/N6B)
To: Department of Defense Inspector General (DoD IG)

Subj: NAVY RESPONSE TO DOD IG PROJECT NO. D2013-0000LC-0142.000

Encl: (1) DoDIG: (b)(7)(E) [redacted]
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10
(11
(12
(13

(14
(15
(16

1. Per reference (a), the following comments are provided:

2. (U) Recommendation A.4

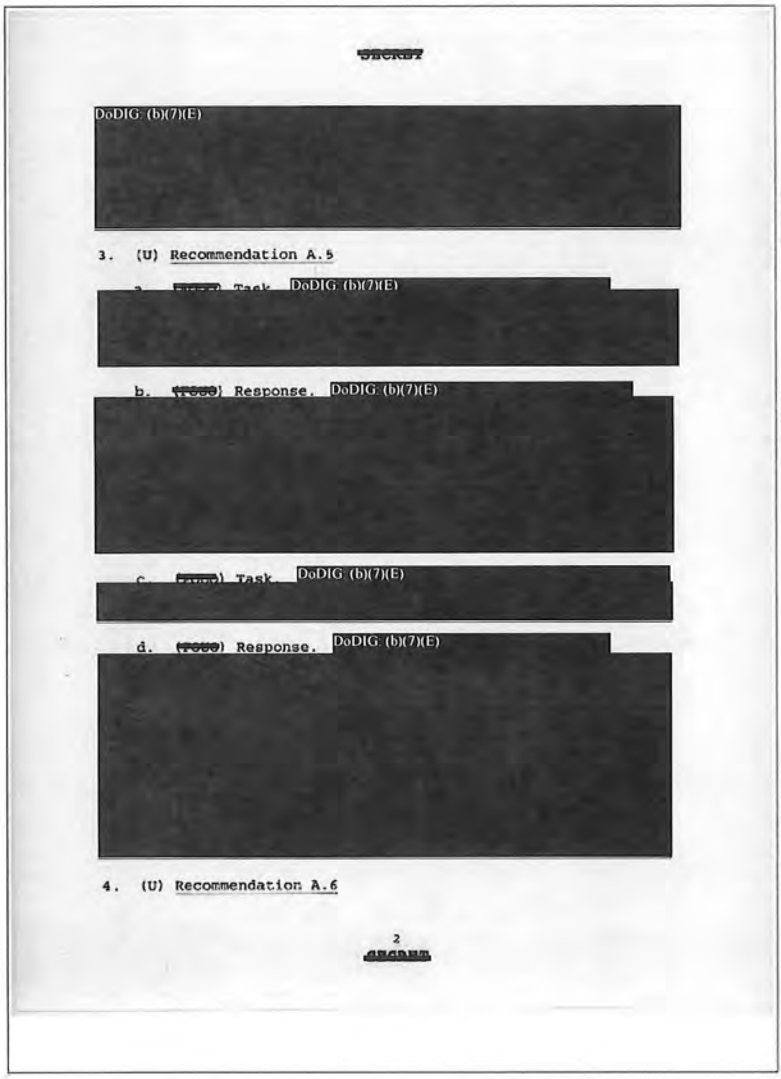
a. (~~[illegible]~~) Task. DoDIG: (b)(7)(E) [redacted]

b. (~~[illegible]~~) Response. DoDIG: (b)(7)(E) [redacted]

~~SECRET~~

(U) Assistant Deputy Chief of Naval Operations, Information Dominance (cont'd)

Final Report Reference



~~SECRET~~

DoDIG (b)(7)(E) [redacted]

Omitted attachments because of length. Copies provided upon request.

3. (U) Recommendation A.5

a. ~~(FOUO)~~ Task. DoDIG (b)(7)(E) [redacted]

b. ~~(FOUO)~~ Response. DoDIG (b)(7)(E) [redacted]

Omitted attachments because of length. Copies provided upon request.

c. ~~(FOUO)~~ Task. DoDIG (b)(7)(E) [redacted]

d. ~~(FOUO)~~ Response. DoDIG (b)(7)(E) [redacted]

Omitted attachments because of length. Copies provided upon request.

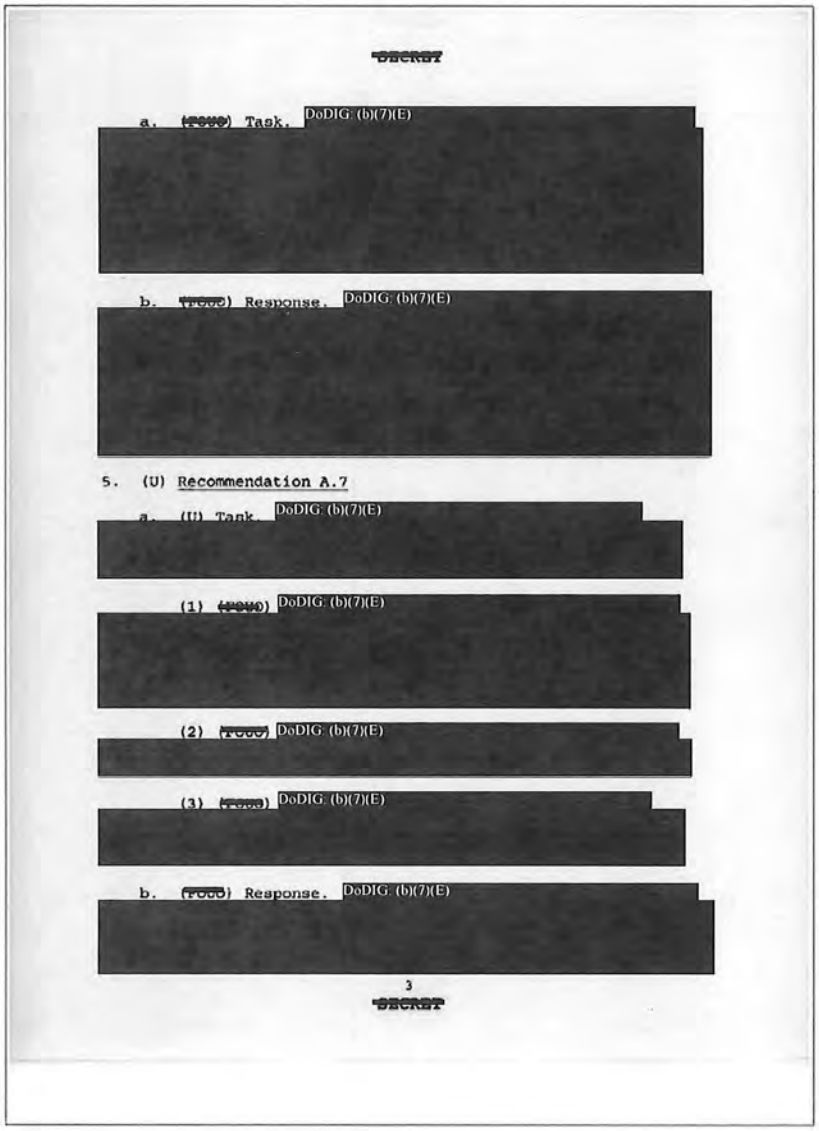
4. (U) Recommendation A.6

2

~~SECRET~~

(U) Assistant Deputy Chief of Naval Operations, Information Dominance (cont'd)

Final Report Reference



~~SECRET~~

a. (~~FOUO~~) Task. DoDIG: (b)(7)(E)

b. (~~FOUO~~) Response. DoDIG: (b)(7)(E)

5. (U) Recommendation A.7

a. (U) Task. DoDIG: (b)(7)(E)

(1) (~~FOUO~~) DoDIG: (b)(7)(E)

(2) (~~FOUO~~) DoDIG: (b)(7)(E)

(3) (~~FOUO~~) DoDIG: (b)(7)(E)

b. (~~FOUO~~) Response. DoDIG: (b)(7)(E)

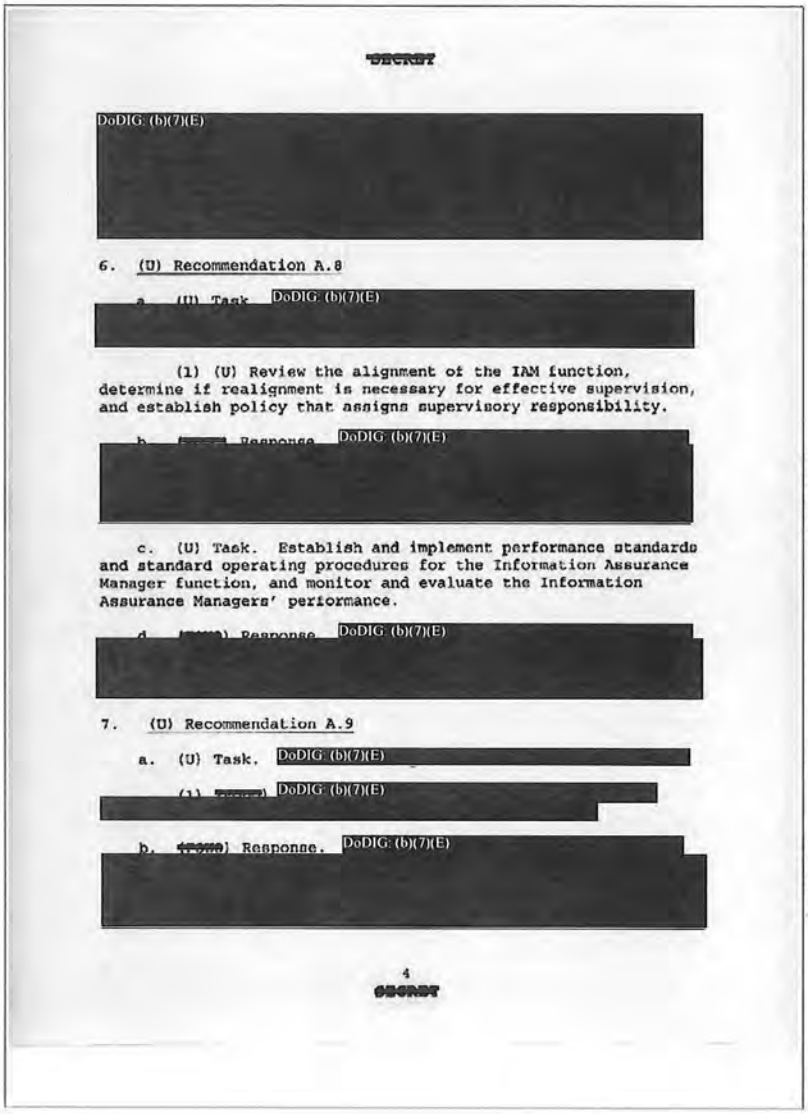
3

~~SECRET~~

Omitted attachments because of length. Copies provided upon request.

(U) Assistant Deputy Chief of Naval Operations, Information Dominance (cont'd)

Final Report Reference



~~SECRET~~

DoDIG: (b)(7)(E) [redacted]

6. (U) Recommendation A.8

a. (U) Task. DoDIG: (b)(7)(E) [redacted]

(1) (U) Review the alignment of the IAM function, determine if realignment is necessary for effective supervision, and establish policy that assigns supervisory responsibility.

b. ~~(FOUO)~~ Response. DoDIG: (b)(7)(E) [redacted]

c. (U) Task. Establish and implement performance standards and standard operating procedures for the Information Assurance Manager function, and monitor and evaluate the Information Assurance Managers' performance.

d. ~~(FOUO)~~ Response. DoDIG: (b)(7)(E) [redacted]

7. (U) Recommendation A.9

a. (U) Task. DoDIG: (b)(7)(E) [redacted]

(1) ~~(FOUO)~~ DoDIG: (b)(7)(E) [redacted]

b. ~~(FOUO)~~ Response. DoDIG: (b)(7)(E) [redacted]

4

~~SECRET~~

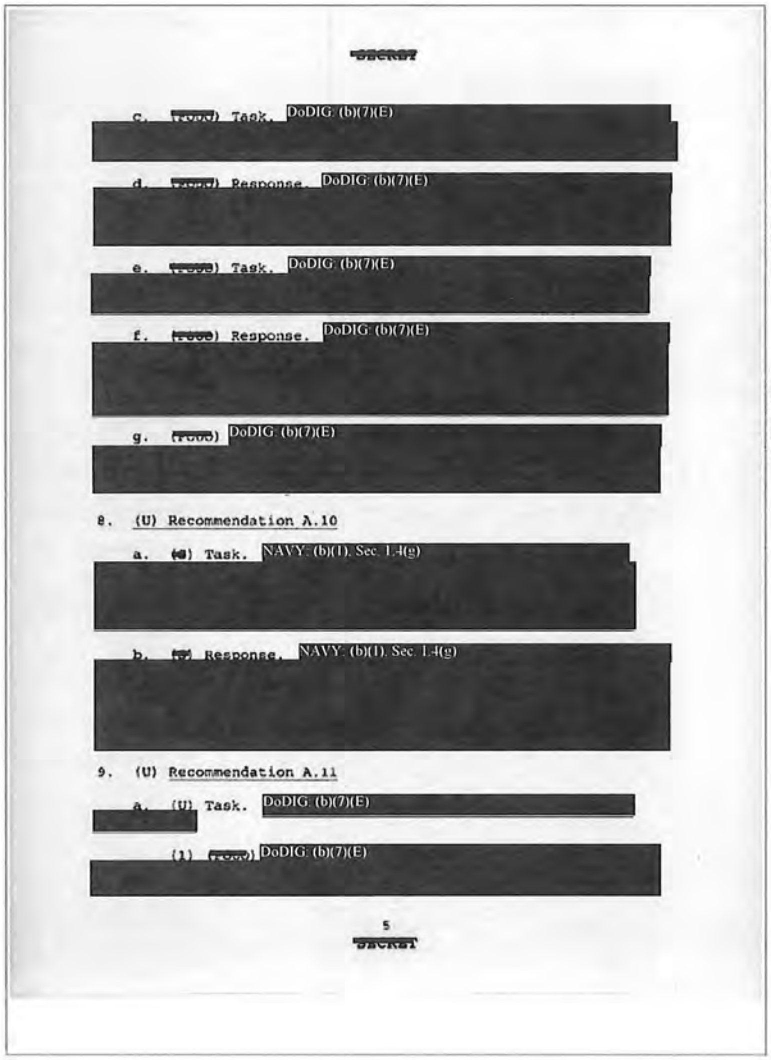
Omitted attachments because of length. Copies provided upon request.

Omitted attachments because of length. Copies provided upon request.

Omitted attachments because of length. Copies provided upon request.

(U) Assistant Deputy Chief of Naval Operations, Information Dominance (cont'd)

Final Report Reference



~~SECRET~~

c. ~~(FOUO)~~ Task. DoDIG: (b)(7)(E)

d. ~~(FOUO)~~ Response. DoDIG: (b)(7)(E)

e. ~~(FOUO)~~ Task. DoDIG: (b)(7)(E)

f. ~~(FOUO)~~ Response. DoDIG: (b)(7)(E)

g. ~~(FOUO)~~ DoDIG: (b)(7)(E)

8. (U) Recommendation A.10

a. ~~(S)~~ Task. NAVY: (b)(1), Sec. 1.4(g)

b. ~~(S)~~ Response. NAVY: (b)(1), Sec. 1.4(g)

9. (U) Recommendation A.11

a. (U) Task. DoDIG: (b)(7)(E)

(1) ~~(FOUO)~~ DoDIG: (b)(7)(E)

5

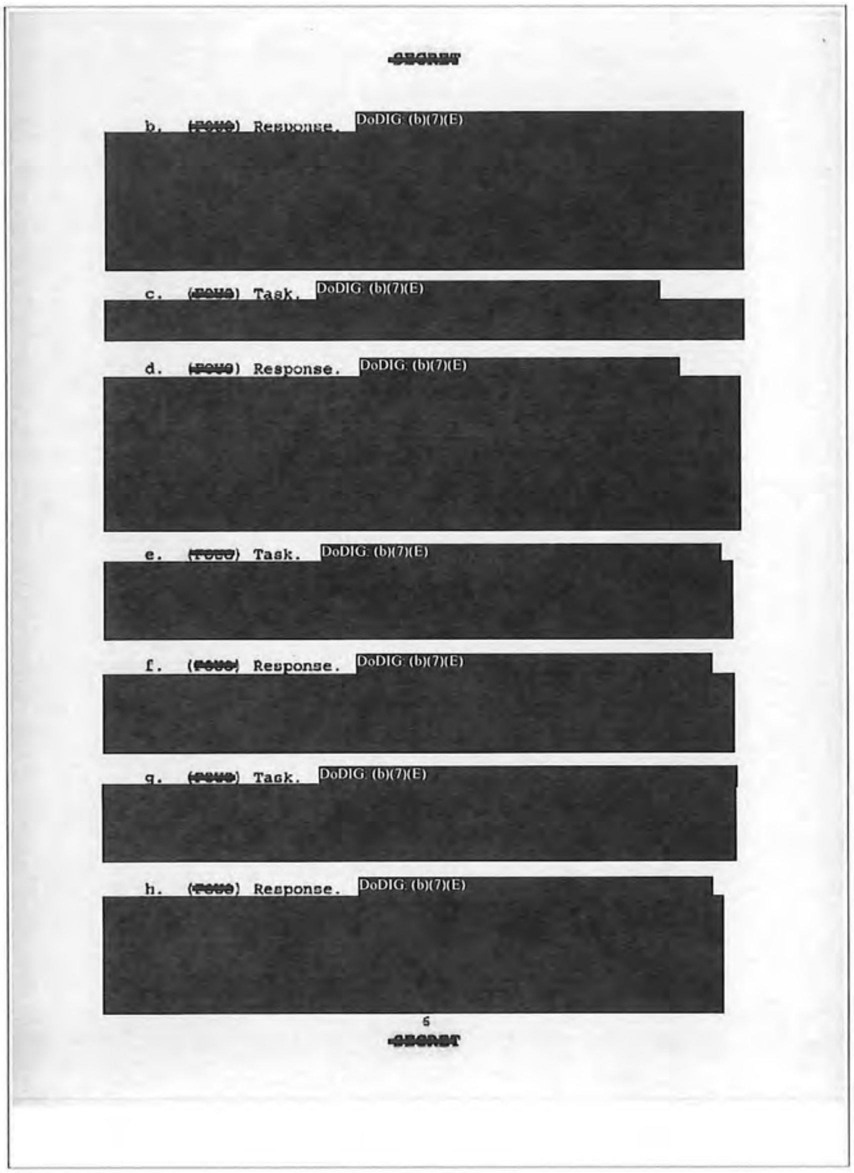
~~SECRET~~

Omitted attachments because of length. Copies provided upon request.

Omitted attachments because of length. Copies provided upon request.

~~SECRET~~

(U) Assistant Deputy Chief of Naval Operations, Information Dominance (cont'd)



~~SECRET~~

b. (~~FOUO~~) Response. DoDIG: (b)(7)(E) [redacted]

c. (~~FOUO~~) Task. DoDIG: (b)(7)(E) [redacted]

d. (~~FOUO~~) Response. DoDIG: (b)(7)(E) [redacted]

e. (~~FOUO~~) Task. DoDIG: (b)(7)(E) [redacted]

f. (~~FOUO~~) Response. DoDIG: (b)(7)(E) [redacted]

g. (~~FOUO~~) Task. DoDIG: (b)(7)(E) [redacted]

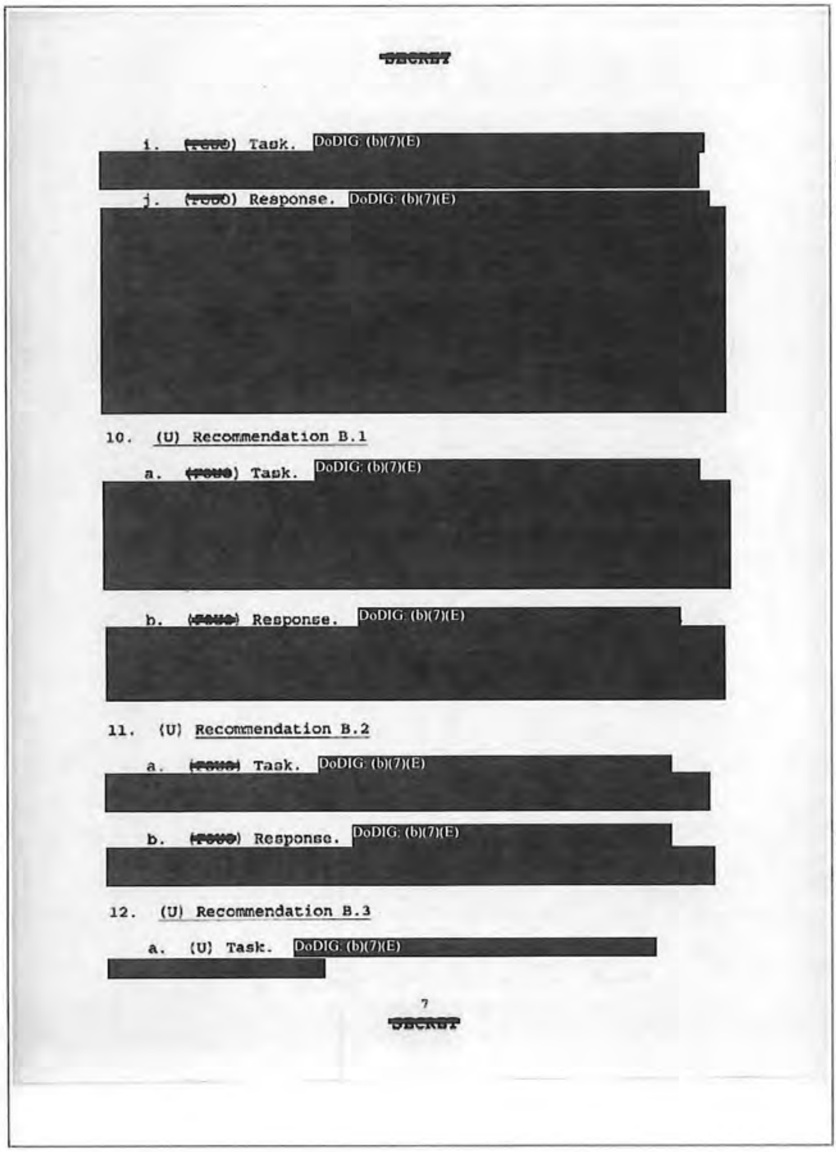
h. (~~FOUO~~) Response. DoDIG: (b)(7)(E) [redacted]

6

~~SECRET~~

(U) Assistant Deputy Chief of Naval Operations, Information Dominance (cont'd)

Final Report Reference



~~SECRET~~

i. (~~FOUO~~) Task. DoDIG: (b)(7)(E) [redacted]

j. (~~FOUO~~) Response. DoDIG: (b)(7)(E) [redacted]

Omitted attachments because of length. Copies provided upon request.

10. (U) Recommendation B.1

a. (~~FOUO~~) Task. DoDIG: (b)(7)(E) [redacted]

b. (~~FOUO~~) Response. DoDIG: (b)(7)(E) [redacted]

11. (U) Recommendation B.2

a. (~~FOUO~~) Task. DoDIG: (b)(7)(E) [redacted]

b. (~~FOUO~~) Response. DoDIG: (b)(7)(E) [redacted]

Omitted attachments because of length. Copies provided upon request.

12. (U) Recommendation B.3

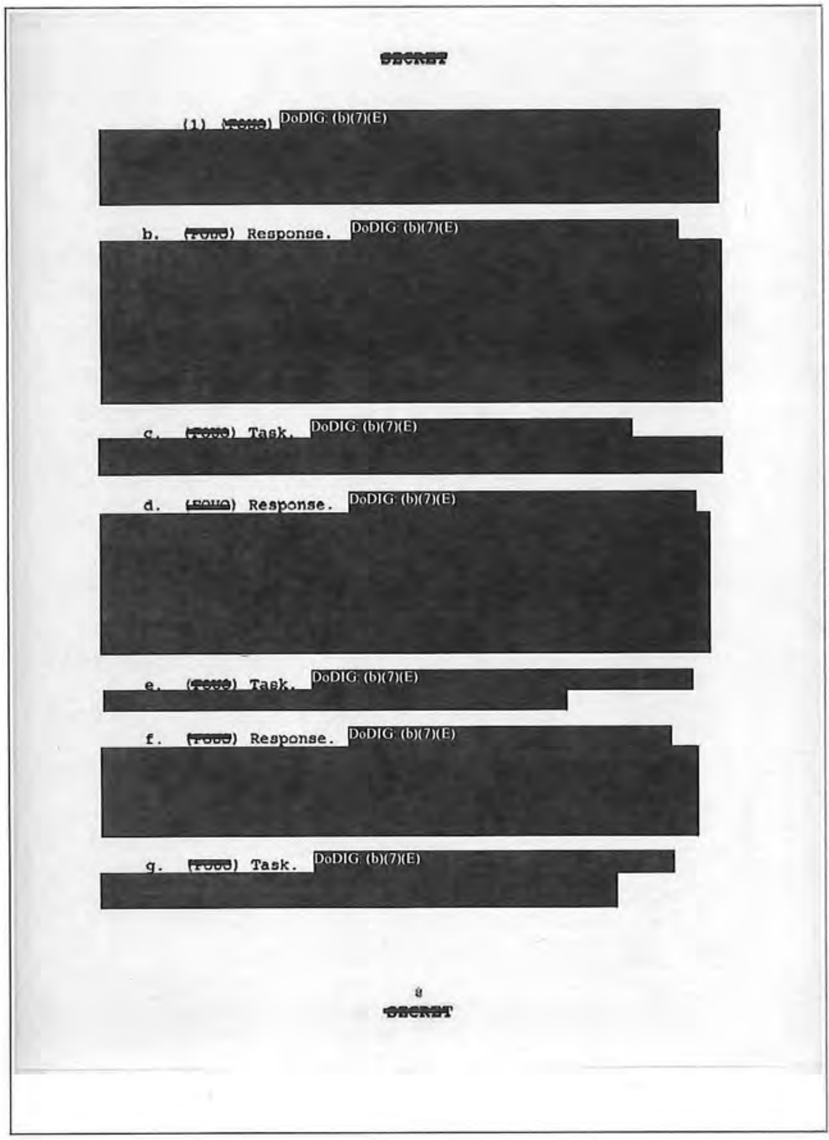
a. (U) Task. DoDIG: (b)(7)(E) [redacted]

7

~~SECRET~~

(U) Assistant Deputy Chief of Naval Operations, Information Dominance (cont'd)

Final Report Reference



~~SECRET~~

(1) (~~FOUO~~) DoDIG: (b)(7)(E) [redacted]

b. (~~FOUO~~) Response. DoDIG: (b)(7)(E) [redacted]

Omitted attachments because of length. Copies provided upon request.

c. (~~FOUO~~) Task. DoDIG: (b)(7)(E) [redacted]

d. (~~FOUO~~) Response. DoDIG: (b)(7)(E) [redacted]

Omitted attachments because of length. Copies provided upon request.

e. (~~FOUO~~) Task. DoDIG: (b)(7)(E) [redacted]

f. (~~FOUO~~) Response. DoDIG: (b)(7)(E) [redacted]

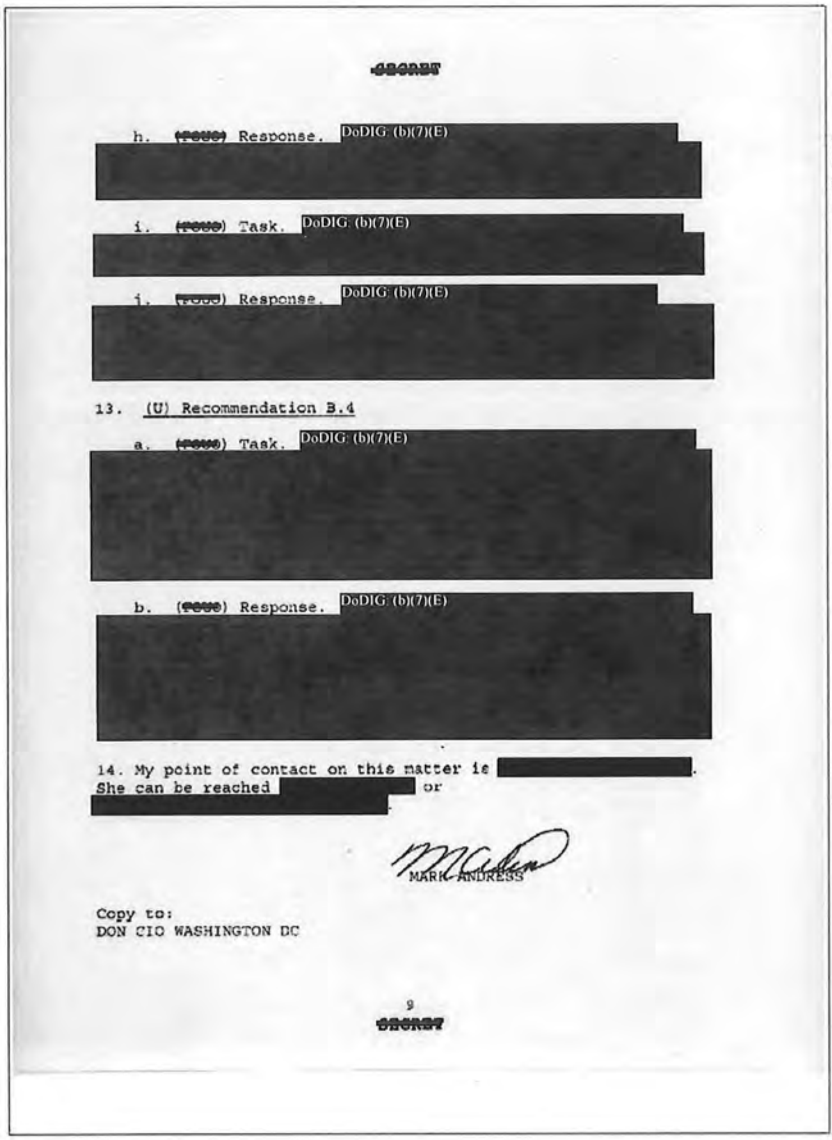
g. (~~FOUO~~) Task. DoDIG: (b)(7)(E) [redacted]

8

~~SECRET~~

(U) Assistant Deputy Chief of Naval Operations, Information Dominance (cont'd)

Final Report Reference



~~SECRET~~

h. (~~FOUO~~) Response. DoDIG: (b)(7)(E) [redacted]

i. (~~FOUO~~) Task. DoDIG: (b)(7)(E) [redacted]

j. (~~FOUO~~) Response. DoDIG: (b)(7)(E) [redacted]

13. (U) Recommendation B.4

a. (~~FOUO~~) Task. DoDIG: (b)(7)(E) [redacted]

b. (~~FOUO~~) Response. DoDIG: (b)(7)(E) [redacted]

14. My point of contact on this matter is [redacted]. She can be reached [redacted] or [redacted]

MARK ANDRESS

Copy to:
DON CIO WASHINGTON DC

9

~~SECRET~~

Omitted attachments because of length. Copies provided upon request.

(U) Glossary

(U) **Accreditation Decision.** A formal statement by a designated accrediting authority regarding acceptance of the risk associated with operating a DoD information system and expressed as an ATO, Interim ATO, Interim Authorization to Test, or Denial of ATO. The accreditation decision may be issued in hard copy with a traditional signature or issued electronically signed with a DoD public key infrastructure–certified digital signature.

(U) **Approval to Connect.** A formal statement by the Connection Approval Office granting approval for an information system to connect to the DISN. The Approval to Connect cannot be granted for longer than the period of validity of the associated ATO. An ATO may be issued for up to 3 years. An Approval to Connect will not be granted based on an Interim ATO.

(U) **Artifacts.** System policies, documentation, plans test procedures, test results and other evidence that express or enforce the IA posture of the DoD information system, make up the certification and accreditation information, and provide evidence of compliance with the assigned IA controls.

(U) **Authorization to Operate (ATO).** Authorization granted by a designated accrediting authority for a DoD information system to process, store, or transmit information; an ATO indicates a DoD information system has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the designated accrediting authority. ATOs may be issued for up to 3 years.

(U) **Category (CAT) I Severity.** Assigned to findings that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumptions of super-user privileges. An ATO will not be granted while CAT I weaknesses are present.

(U) **Category (CAT) II Severity.** Assigned to findings that have a potential to lead to unauthorized system access or activity. CAT II findings that have been satisfactorily mitigated will not prevent an ATO from being granted.

(U) **Certification Determination.** A certifying authority's determination of the degree to which a system complies with assigned IA controls based on validation results. It identifies and assesses the residual risk with operating a system and the costs to correct or mitigate IA vulnerabilities as documented in the IT Security POA&M.

(U) **Classified Transport Boundary.** A physical or logical perimeter of a system that conveys classified information from one location to another and requires protection.

(U) **Cross-Domain Solution.** A form of controlled interface that provides the ability to manually or automatically access and transfer information between different security domains.

(U) **Denial of Authorization to Operate.** A designated accrediting authority decision that a DoD information system cannot operate because of an inadequate IA design, failure to adequately implement assigned IA controls, or other lack of adequate security. If the system is already operational, the operation of the system is halted.

(U) **DIACAP Implementation Plan.** Contains the information system's assigned IA controls. The plan also includes the implementation status, responsible entities, resources, and the estimated completion date for each assigned IA control. The plan may reference applicable supporting implementation material and artifacts.

(U) **DIACAP Scorecard.** A summary report that succinctly conveys information on the IA security posture of a DoD information system in a format that can be exchanged electronically. It shows the implementation status of a DoD information system's assigned IA controls, non compliant, or not applicable as well as the certification and accreditation status.

(U) **Domain.** An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

(U) **Encrypted Tunnel.** An encrypted tunnel sends secure information between networks by encapsulating network protocols within packets.

(U) **Interim Authorization to Operate.** Temporary authorization granted by the designated accrediting authority to operate a DoD information system under the conditions or constraints enumerated in the accreditation decision.

(U) **Network Topology.** Depicts the security posture of the network enclave that will be connecting to the DISN.

(U) **Plan of Action and Milestones (POA&M).** A permanent record that identifies tasks to be accomplished in order to resolve vulnerabilities; required for any accreditation decision that requires corrective actions, it specifies resources required to accomplish the tasks enumerated in the plan and milestones for completing the tasks; also used to document designated accrediting authority accepted non compliant IA controls and baseline IA controls that are not applicable. An IT Security POA&M may be active or inactive throughout a system's life cycle as weaknesses are newly identified or closed.

(U) **Protected Distribution System (PDS).** A system used to transmit encrypted classified National Security Information through an area of lesser classification or control.

(U) **Security Posture.** The security status of an enterprise's networks, information, and systems based on IA resources and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

(U) **Severity Codes.** The category assigned to a system IA vulnerability by a Certifying Authority as part of certification analysis to indicate the risk level associated with the IA vulnerability and the urgency with which the corrective action must be completed. Severity categories are expressed as CAT I, CAT II, or CAT III, with CAT I indicating the greatest risk and urgency.

(U) **System Identification Profile.** A compiled list of system characteristics or qualities required to register an information system with the governing DoD Component IA program.

(U) **Validation.** Confirmation that requirements for a specific intended use or application have been fulfilled.

(U) Annex

(U) Sources

~~(FOUO)~~ Source 1: DoD Instruction O-3600.02, "Information Operations (IO) Security Classification Guide," November 28, 2005 (Document ~~For Official Use Only~~)

~~(FOUO)~~ Source 2: DoDIG: (b)(7)(E) [redacted] (Document classified ~~Secret~~)

Declassify On: 20371105
Date of Source: November 5, 2012

~~(FOUO)~~ Source 3: DoDIG: (b)(7)(E) [redacted] (Document classified ~~Secret~~)

Declassify On: 20371102
Date of Source: November 2, 2012

~~(FOUO)~~ Source 4: DoDIG: (b)(7)(E) [redacted]
(Document classified ~~Secret~~)

Declassify On: 20220323
Date of Source: May 4, 2012

(U) Acronyms and Abbreviations

ATO	Authorization to Operate
CAT	Category
CDSA	Cross-Domain Solution Authorization
CIO	Chief Information Officer
DDCIO(N)	Department of the Navy Deputy Chief Information Officer (Navy)
DIACAP	Defense Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoDI	DoD Instruction
DoDM	DoD Manual
DON	Department of the Navy
DoDIG (b)(7)(E) [redacted]	
IA	Information Assurance
IAM	Information Assurance Manager
IT	Information Technology
NATO	North Atlantic Treaty Organization
NMCI	Navy Marine Corps Intranet
DoDIG (b)(7)(E) [redacted]	
DoDIG (b)(7)(E) [redacted]	
ODAA	Operational Designated Accrediting Authority
PDS	Protected Distribution System
POA&M	Plan of Action and Milestones
SAAR-N	System Access Authorization Request Navy
SIPRNET	Secret Internet Protocol Router Network

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 Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

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

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

Monthly Update
dodigconnect-request@listserve.com

Reports Mailing List
dodig_report@listserve.com

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098