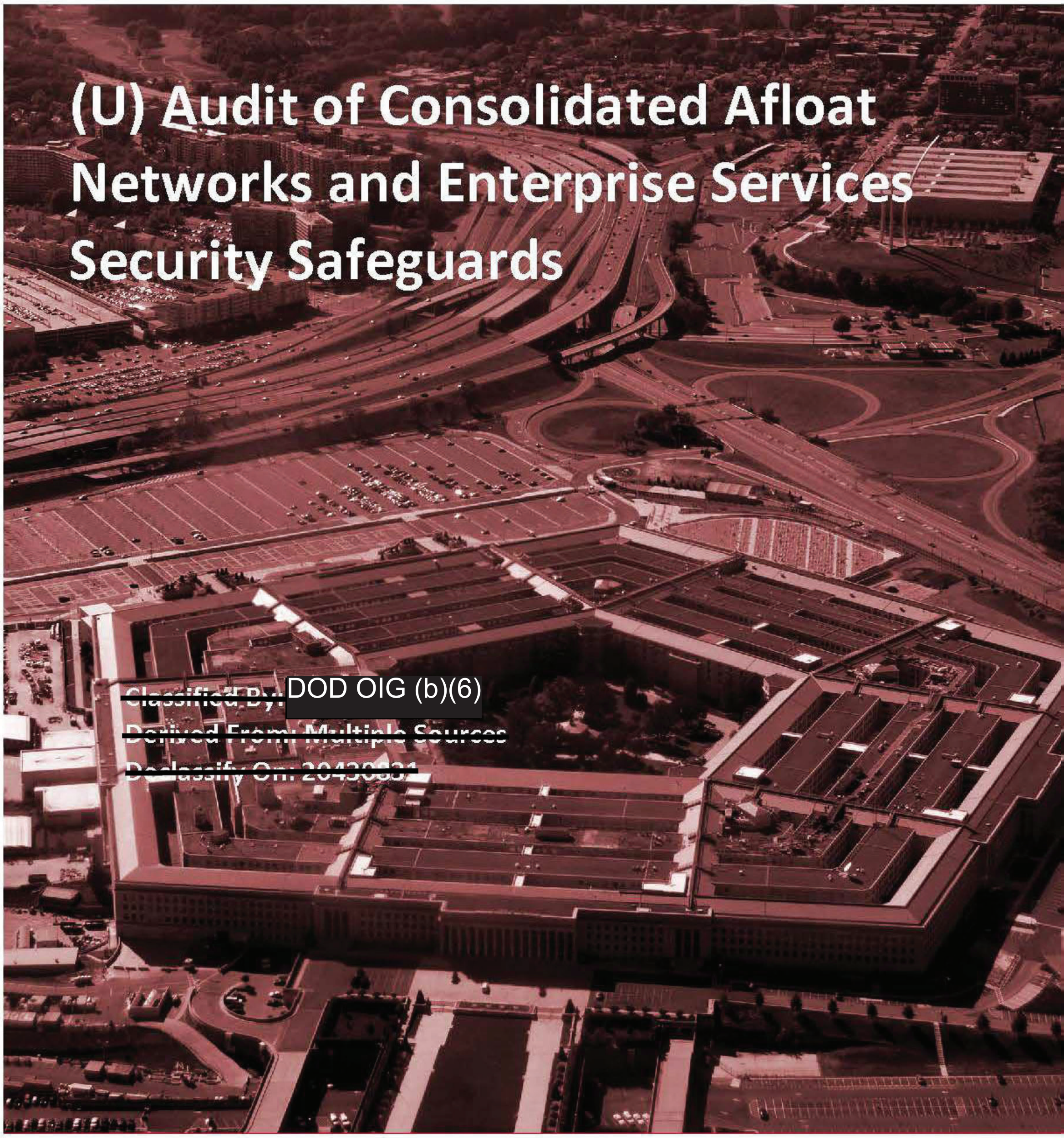
Report No. DODIG-2019-072

~~SECRET~~

INSPECTOR GENERAL

U.S. Department of Defense

APRIL 8, 2019



# (U) Audit of Consolidated Afloat Networks and Enterprise Services Security Safeguards

~~Classified By:~~ DOD OIG (b)(6)
~~Derived From: Multiple Sources~~
~~Declassify On: 20430831~~

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

~~SECRET~~

# (U) Results in Brief

*(U) Audit of Consolidated Afloat Networks and Enterprise Services Security Safeguards*

April 8, 2019

## (U) Objective

(U) We determined whether the Navy implemented security safeguards to protect the Consolidated Afloat Networks and Enterprise Services (CANES) information system from insider and external cyber threats.

## (U) Background

(U) In October 2008, the Deputy Chief of Naval Operations for Communications Networks; the Naval Network Warfare Command (NETWARCOM); and the Program Executive Office Command, Control, Communications, Computers, and Intelligence selected CANES to, among other purposes, reduce the Navy's cybersecurity attack surface (logical access points an adversary could use to gain access) and mitigate network cyber vulnerabilities in a timely manner.

(U) CANES provides ship personnel with inter-ship communications, ship-to-shore communications, and an infrastructure to support communications for tactical and administrative applications. CANES also hosts the Navy's mission-critical system, the Global Command and Control System–Maritime, which is used to provide geographic location information on friendly and hostile land, sea, air, and space forces in the region. As of September 2018, the Navy installed CANES on 67 of the 195 Navy ships that are designated to receive the CANES upgrade.

## (U) Finding

~~(C)~~ NETWARCOM and Program Manager, Warfare 160: Tactical Networks (PMW 160) officials, and CANES administrators aboard the U.S. Ship (USS) *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell* did not implement prescribed cybersecurity controls as mandated by DoD and Navy guidance to protect the CANES network from insider and external cyber threats.

### *(U) Finding (cont'd)*

~~(C)~~ Specifically, they did not:

- ~~(C)~~ mitigate CANES network cyber vulnerabilities;
- ~~(C)~~ [redacted]
- ~~(C)~~ [redacted]
- ~~(C)~~ [redacted]
- ~~(C)~~ identify and account for all CANES-connected devices; or
- ~~(C)~~ [redacted]

~~(C)~~ [redacted]

~~(C)~~ [redacted]

# (U) Results in Brief

## *(U) Audit of Consolidated Afloat Networks and Enterprise Services Security Safeguards*

## (U) Recommendations

~~(S)~~ We recommend that the Chief of Naval Operations, in coordination with the Commanders of the U.S. Fleet Forces and U.S. Pacific Fleet Command and the Program Manager for PMW 160, review the systemic problems identified in this report—including the mitigation of network cyber vulnerabilities in a timely manner, [redacted]—and develop and implement a plan to correct these network and cybersecurity weaknesses.

(U/~~FOUO~~) We also recommend that the Chief of Naval Personnel and the Commander of the Naval Education and Training Command implement a plan to staff ships with the required number of CANES administrators as established by the Chief of Naval Operations.

(U) In addition, we recommend that the Commanding Officers of the USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell*, among other actions:

- ~~(S)~~ [redacted]
- (U//~~FOUO~~) [redacted]
- ~~(S)~~ [redacted]
- (U) revise existing inventory procedures to require all ship personnel to obtain CANES administrator approval before moving devices.

(U//~~FOUO~~) Furthermore, we recommend that the Commander of NETWARCOM, in coordination with the Commanding Officers and Combat Systems Officers for the USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell*, [redacted]. We also recommend that the Commander of NETWARCOM [redacted]

(U//~~FOUO~~) [redacted]

~~(S)~~ Lastly, we recommend that the Program Manager for PMW 160 [redacted]

## (U) Management Comments and Our Response

(U//~~FOUO~~) The Chief of Naval Operations and Commanding Officer of the USS *Abraham Lincoln* did not provide comments on the draft report; therefore, the recommendations are unresolved. Based on comments from the U.S. Pacific Fleet Inspector General on the draft report, we redirected the recommendation to implement a plan to staff the required number of CANES administrators per ship established by the Chief of Naval Operations to the Chief of Naval Personnel and the Commander of the Naval Education and Training Command, who have the authority to correct problems with Navy staffing and training. Therefore, we request comments on the final report from the Chief of Naval Operations, Chief of Naval Personnel, Commander of the Naval Education and Training Command, and the Commanding Officer of the USS *Abraham Lincoln*.

(U//~~FOUO~~) The Program Executive Officer, Command, Control, Communication, Computers, and Intelligence, responding for the Program Manager for PMW 160, agreed with the recommendations [redacted]

# (U) Results in Brief

*(U) Audit of Consolidated Afloat Networks and Enterprise Services Security Safeguards*

### *(U) Management Comments and Our Response (cont'd)*

~~(C)~~ However, the recommendations are unresolved and require additional comments. [redacted]

~~(S)~~ The NETWARCOM Commanding Officer agreed with the recommendations [redacted]. However, the recommendations are unresolved and require additional comments [redacted]

~~(S)~~ The Commodore of Destroyer Squadron Two Eight, responding for the Commanding Officer of the USS *Ramage*, and the Commanding Officers of the USS *Ronald Reagan* and USS *Russell*, agreed with the ~~(S)~~ recommendations [redacted] and requiring all ship personnel to obtain CANES administrator approval before moving devices on the network.

(U) However, two recommendations for the USS *Ronald Reagan* Commanding Officer, two recommendations for the USS *Ramage* Commanding Officer, and one recommendation for the USS *Russell* Commanding Officer are unresolved, and require additional comments. The Commanding Officers need to provide their comments and supporting documentation to show that:

- (U//~~FOUO~~) [redacted]
- (U) crew members completed Operations Security training as required for obtaining and maintaining network access;
- (U//~~FOUO~~) [redacted]
- ~~(S)~~ CANES administrators approved relocating devices before they were moved; and
- (U) they completed monthly inventories of CANES network devices.

(U) Please see the Recommendations Table on the next page.

## *(U) Recommendations Table*

| Unclassified<br>Management | Recommendations Unresolved | Recommendations Resolved | Recommendations Closed |
|---|---|---|---|
| Chief of Naval Operations | 1, 5 | | None |
| Chief of Naval Personnel | 2 | | None |
| Commander, Naval Education and Training Command | 2 | | None |
| Commander, Naval Network Warfare Command | 6, 7 | | None |
| Program Manager, Tactical Networks | 8.a, 8.b | | None |
| Commanding Officer, USS *Abraham Lincoln* | 3.a, 3.b, 3.c, 3.d, 3.e | | None |
| Commanding Officer, USS *Ronald Reagan* | 3.b, 4 | 3.a, 3.c, 3.d, 3.e | None |
| Commanding Officer, USS *Ramage* | 3.d, 4 | 3.a, 3.b, 3.c, 3.e | None |
| Commanding Officer, USS *Russell* | 4 | 3.a, 3.b, 3.c, 3.d, 3.e | None<br>**Unclassified** |

(U) Please provide Management Comments by May 8, 2019.

(U) NOTE: The following categories are used to describe agency management's comments to individual recommendations:

- **(U) Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **(U) Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **(U) Closed** – OIG verified that the agreed upon corrective actions were implemented.

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

April 8, 2019

MEMORANDUM FOR CHIEF OF NAVAL OPERATIONS
CHIEF OF NAVAL PERSONNEL
NAVAL INSPECTOR GENERAL
COMMANDER, NAVAL NETWORK WARFARE COMMAND
COMMANDER, NAVAL EDUCATION AND TRAINING COMMAND

SUBJECT: (U) Audit of Consolidated Afloat Networks and Enterprise Services Security Safeguards (Report No. DODIG-2019-072)

(U) We are providing this report for your review and comment. We conducted this audit in accordance with generally accepted government auditing standards.

(U) We considered management comments on the draft report when preparing the final report. DoD Instruction 7650.03 requires that recommendations be resolved promptly. The Chief of Naval Operations and Commanding Officer of the U.S. Ship *Abraham Lincoln* did not respond to the draft report. Based on management comments, we redirected Recommendation 2 to the Chief of Naval Personnel and the Commander of the Naval Education and Training Command. Therefore, we request that the Chief of Naval Operations, Chief of Naval Personnel, and the Commanding Officer of the U.S. Ship *Abraham Lincoln* provide comments on the final report by May 8, 2019.

(U) Management comments from the Commanding Officer of the Naval Network Warfare Command did not address the specifics of Recommendations 6 and 7. Comments from the Program Executive Officer, Command, Control, Communication, Computers, and Intelligence, responding for the Program Manager, Tactical Networks partially addressed the specifics of Recommendations 8.a and 8.b. Comments from the Commodore of Destroyer Squadron Two Eight, responding for the Commanding Officer of the U.S. Ship *Ramage*; and the Commanding Officers of the U.S. Ships *Ronald Reagan* and *Russell* partially addressed the specifics of Recommendations 3.d and 4 for the U.S. Ship *Ramage*; Recommendations 3.b and 4 for the U.S. Ship *Ronald Reagan*; and Recommendation 4 for the U.S. Ship *Russell*. Therefore, those recommendations are unresolved. We request that the Program Manager and Commanding Officers provide additional comments on those recommendations by May 8, 2019.

(U) Please send a PDF file containing your comments on the recommendations to [redacted]@dodig.smil.mil and [redacted]@dodig.smil.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. Comments provided on the final report must be marked and portion-marked, as appropriate, in accordance with DoD Manual 5200.01.

(U) We appreciate the cooperation and assistance received during the audit. Please direct questions to me at [redacted] (DSN [redacted]).

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General
Cyberspace Operations

# (U) Contents

(U) Introduction....................1

(U) Objective....................1

(U) Background....................1

(U) Review of Internal Controls....................5

(U) Finding....................6

(U) Cybersecurity Controls to Protect the CANES Network Were Not Implemented....................6

(U) Cybersecurity Controls Were Not Implemented....................7

(U//~~FOUO~~) CANES Administrator Staffing Was Insufficient to Operate, Maintain, or Protect the Network....................23

(U//~~FOUO~~) Security Weaknesses May Compromise the CANES Network....................24

(U) Management Comments on the Finding and Our Response....................25

(U) Recommendations, Management Comments, and Our Response....................25

(U) Appendix A....................41

(U) Scope and Methodology....................41

(U) Use of Computer-Processed Data....................44

(U) Use of Technical Assistance....................45

(U) Prior Coverage....................45

(U) Appendix B....................46

(U) Roles and Responsibilities....................46

(U) Appendix C....................48

(U) Ships with CANES....................48

(U) Appendix D....................52

(U) Management Comments on the Finding and Our Response....................52

(U) Management Comments....................55

(U) U.S. Pacific Fleet....................55

(U) Program Executive Officer, Command, Control, Communication, Computers, and Intelligence....................57

(U) Naval Network Warfare Command....................59

(U) Destroyer Squadron Two Eight....................61

(U) USS *Ronald Reagan*....................62

(U) USS *Russell*....................65

(U) Source of Classified Information....................77

(U) Acronyms and Abbreviations....................78

(U) Glossary....................79

# (U) Introduction

## (U) Objective

(U) We determined whether the Navy implemented security safeguards to protect the Consolidated Afloat Networks and Enterprise Services (CANES) information system from internal and external threats.

## (U) Background

(U) In October 2008, the Deputy Chief of Naval Operations for Communications Networks; the Naval Network Warfare Command (NETWARCOM); and the Program Executive Office Command, Control, Communications, Computers, and Intelligence selected CANES to reduce the Navy's cybersecurity attack surface, mitigate network cyber vulnerabilities in timely manner, improve system management and detection capabilities for addressing cybersecurity risks, and modernize ship architectures using up-to-date operating systems.[1] CANES consists of integrated commercial off the-shelf software, hardware, and firmware, and supports application hosting and service delivery for the Navy afloat environment. The Navy is fielding CANES to replace the following five shipboard networks, which the Navy used to support shipboard communications and network capabilities.

- (U) Sensitive Compartmented Information Networks
- (U) Integrated Shipboard Network System
- (U) Submarine Local Area Network
- (U) Combined Enterprise Regional Information Exchange Systems-Maritime
- (U) Video Information Exchange System

(U) CANES also hosts the Navy's mission-critical system, the Global Command and Control System–Maritime.[2] Navy commanders use the Global Command and Control System–Maritime to increase the commander's situational awareness through detailed geographic information on friendly and hostile land, sea, air, and space forces.

[1] (U) Attack surface refers to different logical access points that adversaries can use to gain access to a network or system and exfiltrate (steal) data.

[2] (U) Mission critical systems are systems that process information that the loss, misuse, disclosure, unauthorized access, or modification of would have debilitating impact on an agency's mission.

## *(U) CANES Architecture*

(U) CANES provides ship personnel with inter-ship communications, ship-to-shore communications, and an infrastructure to support communications for tactical and administrative applications. CANES also provides voice, video, and e-mail capabilities and Internet access to the Non-Classified Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet), and the Joint Worldwide Intelligence Communications System (Top Secret/Sensitive Compartmented Information security environment) using enclaves that are separately protected within the CANES network.[3]

(U) The CANES architecture includes virtual servers, workstations, printers, and Voice over Internet Protocol communications that operate with Microsoft Windows 7 or Microsoft Windows 10 operating systems, depending on the software release. The CANES architecture is protected by security devices, such as network boundary firewalls, intrusion prevention systems, routers, and switches.[4] The Navy last accredited CANES under the DoD Information Assurance Certification and Accreditation Program in March 2017.[5] As of October 2018, the Navy was in the process of accrediting CANES based on DoD Risk Management Framework requirements and expected to complete the process in September 2019.

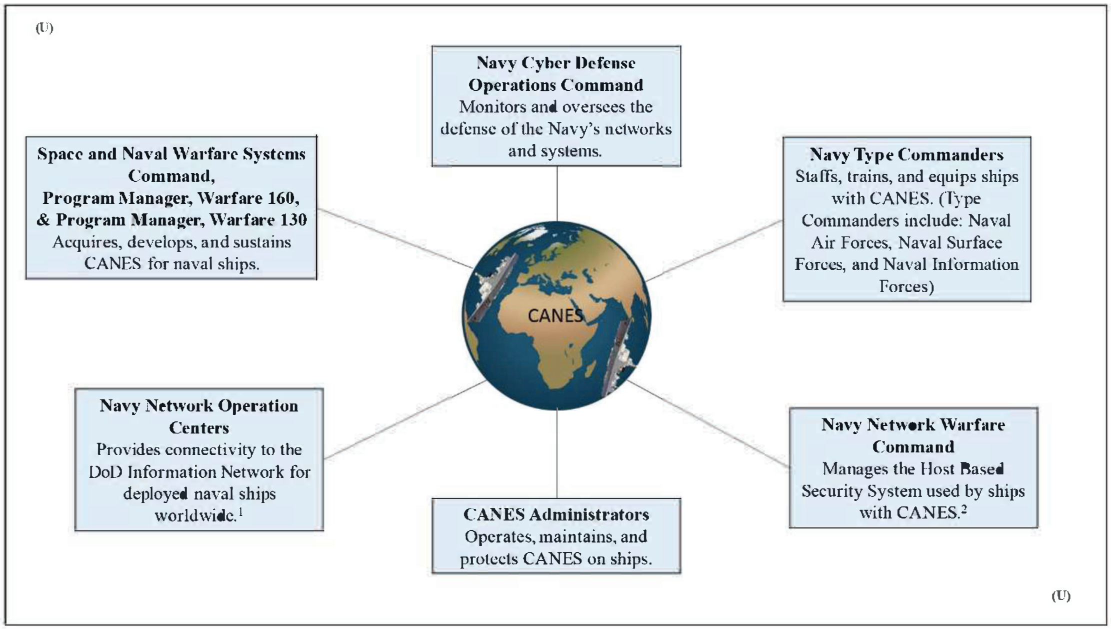
(U) As illustrated in Figure 1, several Navy commands and functional specialists are responsible for operating, maintaining, and protecting CANES. See Appendix B for their specific roles and responsibilities.

[3] (U) Enclaves are a set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

[4] (U) Network boundary firewalls are security devices that limit access between logical perimeters of a network. Intrusion prevention systems are security devices that detect unusual or malicious activities and attempt to stop detected possible incidents. Routers are security devices that analyze the content of information transmitted within or between networks. Switches are security devices that receive and redirect incoming network traffic to specific areas within the network.

[5] (U) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Program (DIACAP)," November 28, 2007. DoD Instruction 8510.01 was replaced and reissued as DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014 (updated July 28, 2017). Although replaced, DoD Components are subject to the requirements in the DoD Information Assurance Certification and Accreditation Program until the system or network is accredited under the DoD Risk Management Framework.

*(U) Figure 1. Key Stakeholders Responsible for Operating, Maintaining, and Protecting CANES*


(U)
Navy Cyber Defense Operations Command
Monitors and oversees the defense of the Navy's networks and systems.
Space and Naval Warfare Systems Command, Program Manager, Warfare 160, & Program Manager, Warfare 130
Acquires, develops, and sustains CANES for naval ships.
Navy Type Commanders
Staffs, trains, and equips ships with CANES. (Type Commanders include: Naval Air Forces, Naval Surface Forces, and Naval Information Forces)
CANES
Navy Network Operation Centers
Provides connectivity to the DoD Information Network for deployed naval ships worldwide.1
Navy Network Warfare Command
Manages the Host Based Security System used by ships with CANES.2
CANES Administrators
Operates, maintains, and protects CANES on ships.
(U)

[1] (U) The DoD Information Network is the DoD's portion of the Internet.

[2] (U) Host Based Security Systems include a suite of centrally-managed Defensive Cyber Operations tools that enables the Navy to prevent, detect, track, report, and remediate malicious computer-related activities and incidents.

(U) Source: The DoD Office of Inspector General (DoD OIG).

(U) Aboard Navy ships, CANES administrators report to the Combat Systems Officer and are responsible for operating, maintaining, and protecting the CANES network. Their responsibilities include:

- (U) correcting and mitigating CANES network cyber vulnerabilities;
- (U) establishing, maintaining, and managing CANES user accounts; and
- (U) reviewing and managing log files for indications of unauthorized access and unusual or malicious behavior within the network.

## (U) CANES Implementation Timeline

(U) The Navy plans to install CANES on 195 ships by September 2024. In January 2014, the Program Manager, Warfare 160: Tactical Networks (PMW 160), and the Space and Naval Warfare Systems Command (SPAWAR) completed the first CANES installation on U.S. Ship (USS) *Milius*. As of September 2018, PMW 160 had installed CANES on 67 ships. See Appendix C for a list of the 67 ships, the installation dates, and the CANES version installed on each ship.

(U) To meet the specific networking needs of different ship classes, PMW 160 and SPAWAR developed three variations of CANES:

- (U) Unit-level for smaller ships, such as destroyers and cruisers,
- (U) Force-level for larger ships, such as aircraft carriers and amphibious assault ships, and
- (U) Submarine for ballistic and nuclear submarines.[6]

(U) PMW 160 and SPAWAR also provide ships with periodic upgrades for CANES hardware and software. Key deployment milestones for CANES are listed below.

- (U) **October 2008:** The Chief of Naval Operations approved CANES deployment.
- (U) **January 2014:** CANES was first installed on a Unit level ship, the USS *Milius*.
- (U) **October 2014:** CANES was first installed on a Force level ship, the USS *John C. Stennis*.
- (U) **December 2014:** CANES was first installed on a submarine, the USS *Maryland*.
- (U) **FYs 2014 and 2015:** CANES hardware version 1 and software versions 1.0.0.3, 1.0.0.4, 1.0.0.6, and 1.0.0.9 were fielded on 31 Unit level and 9 Force-level ships.
- (U) **FY 2015 through Present:** CANES hardware versions 0 and 1.1 and software versions 0 and Operation Rolling Tide were fielded on 13 submarines.
- (U) **FY 2016 through Present:** CANES hardware version 1.1 and software versions 1.0.1, 1.2, and 2.0 were fielded on eight Unit-level and six Force level ships.

## *(U) Communications Afloat*

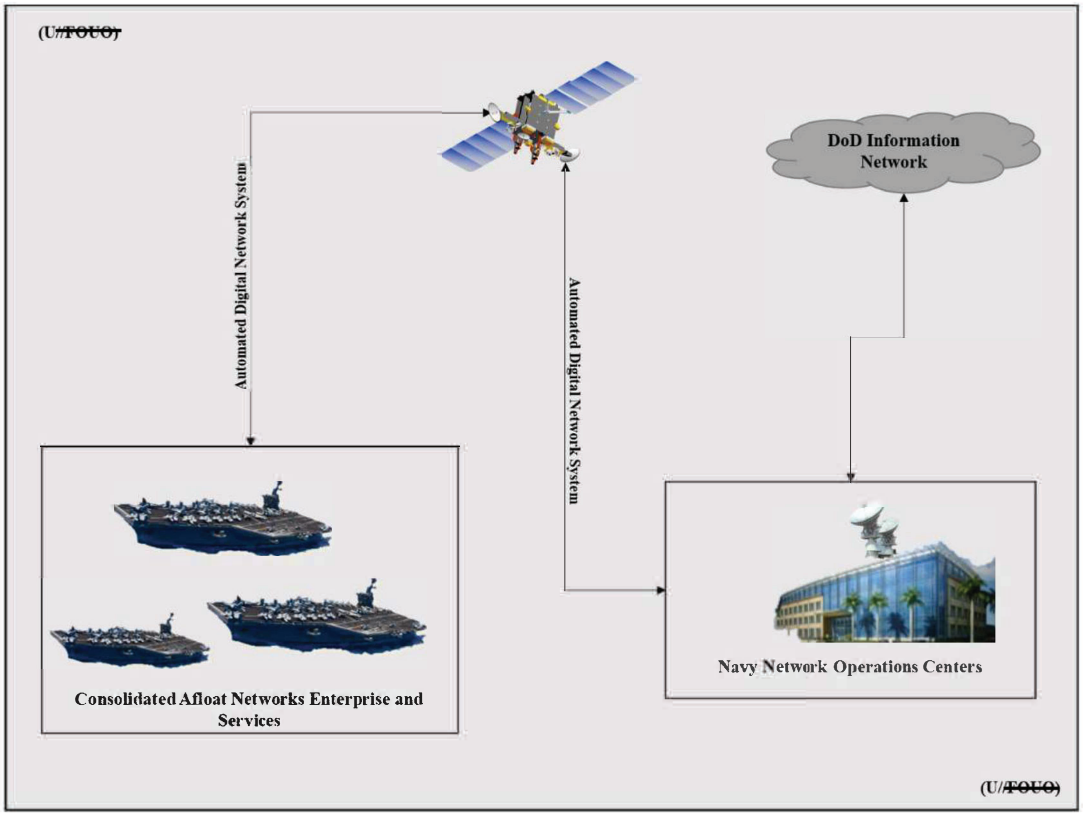
(U) As illustrated in Figure 2, CANES uses the Navy's Automated Digital Network System to transmit encrypted data to other ships and shore locations, including data transfers from deployed ships using the DoD Information Network.[7] Based on the ship's location, the Automated Digital Network System transfers data to one of the four Navy Network Operations Centers; the data is then routed through the DoD Information Network.[8]

[6] (U) We did not review the submarine variant of CANES as part of this audit.

[7] (U) The Automated Digital Network System provides connectivity to surface ships and submarines.

[8] (U) The four Navy Network Operations Centers are located in Wahiawa, Hawaii; Norfolk, Virginia; Naples, Italy; and Manama, Bahrain.

*(U) Figure 2. Communication Afloat*


(U//~~FOUO~~)
Automated Digital Network System
DoD Information Network
Automated Digital Network System
Consolidated Afloat Networks Enterprise and Services
Navy Network Operations Centers
(U//~~FOUO~~)

(U) Source: The DoD OIG.

## (U) Review of Internal Controls

(U//~~FOUO~~) DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[9] We identified Navy-wide internal control weaknesses relating to operating, maintaining, and protecting the Navy's afloat networks. Specifically, security controls were not effective to mitigate network vulnerabilities, [redacted], account for all CANES connected devices, [redacted] We will provide a copy of the report to the senior officials responsible for internal controls at the Chief of Naval Operations; U.S. Fleet Forces Command; U.S. Pacific Fleet; NETWARCOM; PMW 160; and the USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell*.

[9] (U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

# (U) Finding

## (U) Cybersecurity Controls to Protect the CANES Network Were Not Implemented

~~(C)~~ NETWARCOM and PMW 160 officials and CANES administrators aboard the USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell* did not implement cybersecurity controls to protect the CANES network from insider and external cyber threats. Specifically, they did not:

- ~~(C)~~ mitigate cyber network vulnerabilities in a timely manner;
- ~~(C)~~ [redacted]
- ~~(C)~~ [redacted]
- ~~(C)~~ [redacted]
- ~~(C)~~ identify and account for all CANES-connected devices; or
- ~~(C)~~ [redacted].[10]

~~(C)~~ [redacted]

~~(C)~~ [redacted]

[10] (U) Devices include workstations, servers, and laptops. Removable media are items such as compact discs, digital video discs, secure digital cards, flash memory data storage devices, multi-media cards, and external hard drives. Security devices include routers, switches, and firewalls.

~~(C)~~ [redacted]

## (U) Cybersecurity Controls Were Not Implemented

(U//~~FOUO~~) [redacted]. The CANES network supports command and control and communications critical to the ships' missions. NETWARCOM and PMW 160 officials and CANES administrators aboard the USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell* did not implement cybersecurity controls [redacted]. To determine whether the Navy protected the CANES network, we analyzed cybersecurity controls and technologies (tools) the CANES administrators used to manage network access and connected devices, identify and mitigate network cyber vulnerabilities, and monitor data transfers.

(U//~~FOUO~~) Navy (b)(1)(1.7e) [redacted]

(U//~~FOUO~~) The CANES architecture uses similar hardware and software on each type of ship and the ships face similar challenges staffing trained and certified CANES administrators to operate, maintain, and protect the CANES network. The security problems we identified in this report—including mitigating network cyber vulnerabilities in a timely manner, [redacted], accounting for CANES-connected devices, and [redacted]—may also affect other ships with CANES. Therefore, the Chief of Naval Operations, in coordination with the U.S. Fleet Forces Command and the U.S. Pacific Fleet Commanders and PMW 160 Program Manager, should review the systemic problems identified in this report, and develop and implement a plan of action and milestones to ensure that network and cybersecurity weaknesses are corrected on all ships with CANES.

### *(U//~~FOUO~~) PMW 160 and CANES Administrators Did Not Consistently Mitigate Vulnerabilities*

(U//~~FOUO~~) CANES administrators aboard the USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell* did not mitigate known network vulnerabilities [redacted]

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~) Chairman of the Joint Chiefs of Staff Manual 6510.02 requires DoD Components to take corrective actions to mitigate vulnerabilities and develop a plan of action and milestones when they are unable to mitigate vulnerabilities, including information assurance vulnerability alerts, by specified mitigation dates.[12] Information assurance vulnerability alerts, which are issued by U.S. Cyber Command, are notifications generated when vulnerabilities may result in an immediate and potentially severe threat to DoD systems and networks that require corrective actions based on the severity of the risk.

(U//~~FOUO~~) We compared vulnerability network scan results from April through July 2018 for the USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell*, and found that [redacted]. DoD Instruction 8510.01 requires DoD Components to mitigate Category I (CAT I) vulnerabilities within 30 days and CAT II vulnerabilities within 90 days or request approval from the Component's Chief Information Officer to continue to operate the system with unmitigated CAT I vulnerabilities.[13] The DoD uses plans of action and milestones to report unmitigated network cyber vulnerabilities. PMW 160 and CANES administrators aboard the USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell* did not take corrective actions to mitigate vulnerabilities in accordance with DoD requirements, [redacted]. Table 1 lists the number of unmitigated vulnerabilities that the CANES administrators were responsible for patching on the four Navy ships visited.

[11] (U) Plans of action and milestones are permanent records that identify tasks to resolve vulnerabilities and are required for any accreditation decision that requires corrective actions. A plan of action and milestones specifies resources required to complete the tasks to mitigate a vulnerability. It is also used to document designated accrediting authority decisions to accept noncompliant security controls and define security controls that are not applicable to a specific system or network.

[12] (U) Chairman of the Joint Chiefs of Staff Manual 6510.02, "Information Assurance Vulnerability Management (IAVM) Program," November 5, 2013.

[13] (U) CAT I vulnerabilities, if exploited by unauthorized users, could allow unauthorized personnel to bypass primary security protections and gain immediate network access, and therefore require immediate patches. CAT II vulnerabilities, if exploited by unauthorized users, could result in unauthorized network access or activity.

*~~(S)~~ Table 1.  Unmitigated Vulnerabilities That CANES Administrators Were Responsible for Patching on the Ships Visited*

Navy (b)(1)(1.4g)

[redacted]

|  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  | ~~SECRET~~ |

[1] (U) The vulnerability scan results did not identify any unmitigated CAT III vulnerabilities.

[2] (U) The USS *Abraham Lincoln* could not provide the May vulnerability scan for the SIPRNet or the July vulnerability scan for the NIPRNet.

(U) Source:  April through July 2018 Vulnerability Scan Results from the Vulnerability Remediation Asset Manager database.

~~(S)~~ [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

(U//~~FOUO~~) [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

## *(U//~~FOUO~~)* [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

[14] (U) We could not test whether the USS *Russell* properly [redacted], and accounted for network-connected devices on the SIPRNet because of network outages during our visit.

[15] (U//~~FOUO~~) U.S. Cyber Command Communications Tasking Order 14-0185, "Insider Threat Mitigation," July 17, 2014. Write privileges refers to permissions granted to a user or device to transfer data to an object such as removable media.

[16] (U) Naval Information Forces, "U.S. Navy Host Based Security System (HBSS) ePolicy Orchestrator (ePO) Afloat Consolidation Concept of Operations (CONOPS)," September 2015.

~~(S)~~ [redacted][17]

~~(S)~~ [redacted]

## (U//~~FOUO~~) [redacted]

~~(S)~~ [redacted]

[17] (U) We performed control tests, which are audit procedures designed to evaluate the operating effectiveness of controls. When performing the control tests, we used the control test table developed by the DoD OIG Quantitative Methods Division and published in the Council of the Inspectors General on Integrity and Efficiency, "Journal of Public Inquiry," 2012-2013.

~~(S)~~ [redacted]

(U) To test whether devices had antivirus software, we selected a random sample of devices, such as servers and workstations, and observed ship personnel log into the devices to access the [redacted] software program. Specifically, we tested for the existence of antivirus software on devices used aboard the USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell*. Table 2 identifies [redacted].

*~~(S)~~ Table 2.* [redacted]

[redacted]

(U) Source: The DoD OIG.

~~(S)~~ [redacted]

[18] (U) Secretary of the Navy Manual 5239.1, "Department of the Navy Information Assurance Program," November 2005.

~~(S)~~ [redacted]

## *(U//~~FOUO~~)* [redacted]

(U//~~FOUO~~) [redacted]

**(U//~~FOUO~~) Increasing malicious actors' ability to compromise the CANES network.**

(U) [redacted]

[19] (U) Secretary of the Navy Instruction 5230.15, "Information Management/Information Technology Policy for Fielding of Commercial Off-the-Shelf Software," April 10, 2009. [redacted].

~~(S)~~ Navy (b)(1)(1.4g) [redacted]

~~(S)~~ Navy (b)(1)(1.4g) [redacted]

**~~(S)~~ We believe this is a systemic problem that affects the entire CANES program.**

[20] (U) Navy (b)(1)(1.7e) [redacted].

## (U) CANES Administrators Did Not Account For All Network Connected Devices

(U) CANES administrators aboard the USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell* could not identify all NIPRNet- and SIPRNet-connected devices on the CANES network. DoD Instruction 5000.64 requires DoD Components to maintain physical accountability for 98 percent of unclassified information technology devices and 100 percent of classified information technology devices.[21] In addition, Chairman of the Joint Chiefs of Staff Instruction 6510.01F requires information systems to be monitored to detect and react to incidents, intrusions, disruptions of services, or other unauthorized activities that threaten the security of DoD operations.[22]

(U) To test whether CANES administrators could identify and locate network-connected devices, we selected a random sample of NIPRNet and SIPRNet devices, such as servers and workstations; reviewed procedures and technologies used to identify unauthorized CANES network-connected devices; conducted a physical inventory to locate each device in the sample; and compared each device's serial number, workstation number, or media access control address to the ship's physical inventory or Active Directory reports.[23] We identified the following while testing NIPRNet and SIPRNet devices from the USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell*.

- (U) CANES administrators on the USS *Abraham Lincoln* located the 33 SIPRNet-connected servers in our sample, but could not locate 23 of 44 (52 percent) NIPRNet-connected workstations and servers and 22 of 32 (69 percent) SIPRNet-connected workstations in our sample.
- (U) CANES administrators on the USS *Ronald Reagan* located the 17 NIPRNet-connected and 33 SIPRNet-connected servers in our sample, but could not locate 8 of 44 (18 percent) NIPRNet-connected, 11 of 44 (25 percent) NIPRNet-connected embarkable devices, and 9 of 41 (22 percent) SIPRNet-connected workstations in our sample.[24]

[21] (U) DoD Instruction 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property," July 21, 2017.

[22] (U) Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," June 9, 2015.

[23] (U) We developed samples using physical inventory reports from the USS *Abraham Lincoln*, USS *Ronald Reagan*, and USS *Russell* and Active Directory from the USS *Ramage*.

[24] (U) Embarkable devices, such as laptops, are devices brought onto a ship by an individual or unit that connect to the DoD Information Network through a separate CANES enclave.

- (U) CANES administrators on the USS *Ramage* could not locate 24 of 38 (63 percent) NIPRNet-connected and 6 of 35 (17 percent) SIPRNet-connected workstations and servers in our sample.
- (U) CANES administrators on the USS *Russell* could not locate 11 of 36 (31 percent) NIPRNet-connected workstations and servers in our sample.

(U) Although the ships had procedures for conducting periodic inventories and identifying unauthorized devices connected to the network, the CANES administrators did not have accountability of all CANES network-connected devices because the ships did not have procedures that required ship personnel to request administrator approval before physically relocating devices.

(U) When CANES administrators do not maintain full accountability of CANES network-connected devices, they increase the risk of unauthorized access to devices that support critical network functions, such as ship communications. In addition, the CANES administrators reduce their ability to determine whether devices received security configuration updates needed to protect the network from insider and external threats. Furthermore, the CANES administrators reduce their ability to promptly respond to security incidents when they need to physically search the ships for affected devices. The USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell* Commanding Officers, in coordination with the ships' Combat Systems Officers, should revise and implement existing inventory procedures to require all ship personnel to request administrator approval before relocating devices, and perform monthly reviews to identify the location of all network devices.

## *(U)* [redacted]

~~(C)~~ [redacted]

[25] (U) Defense Information Systems Agency, "Enclave Security Technical Implementation Guide," version 4, release 5, August 21, 2014.

[26] (U) National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," revision 4, April 2013.

~~(C)~~ [redacted][28]

(U) DoD guidance requires personnel to complete Operations Security training annually; however, beginning in FY 2019, the Navy began making Operations Security training optional by allowing commanders to determine the need for completing the training.[29] The FY 2019 Navy guidance conflicts with DoD Manual 5205.02, which requires all personnel complete annual Operations Security training. The Chief of Naval Operations should reissue guidance to require all Navy personnel to complete the Operations Security training annually to ensure that users are aware of and understand their responsibilities for safeguarding sensitive and classified information.

~~(S)~~ [redacted][30]

~~(S)~~ [redacted]

[27] (U) The Navy used Office of the Chief of Naval Operations Form 5239/14, "System Authorization Access Request-Navy," September 2011, instead of DD Form 2875.

[28] (U) Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," June 9, 2015. Secretary of the Navy Instruction 3070.2, "Operations Security," May 5, 2016.

[29] (U) Naval Administrative Message 226/18, "FY19 General Military Training Requirements," September 12, 2018.

[30] (U) Defense Information Systems Agency, "Windows 7 Security Technical Implementation Guide," version 1, release 30, April 27, 2018.

~~(S)~~ [redacted]

- ~~(S)~~ [redacted]
- ~~(S)~~ [redacted]

~~(S)~~ [redacted]

- ~~(S)~~ [redacted]
- ~~(S)~~ [redacted]

[31] (U) The SECRET releasable enclave resides on the SIPRNet, but is partitioned to allow only users approved to access SECRET releasable information.

- ~~(S)~~ [redacted]
- ~~(S)~~ [redacted]

~~(S)~~ [redacted]

- ~~(S)~~ [redacted]
- ~~(S)~~ [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

~~(S)~~ [redacted]

- ~~(S)~~ [redacted]
- ~~(S)~~ [redacted]

~~(C)~~ [redacted]

- ~~(C)~~ [redacted]
- ~~(C)~~ [redacted]
- ~~(C)~~ [redacted]
- ~~(C)~~ [redacted]

~~(C)~~ [redacted]

~~(C)~~ [redacted] In addition, the USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell* Commanding Officers, in coordination with the ships' Combat Systems Officers, should review and reconcile whether all personnel assigned to each ship have completed Operations Security training and cyber awareness training, and require personnel who have not completed the training to immediately complete the annual security-related training.

[redacted]

## (U//~~FOUO~~) CANES Administrator Staffing Was Insufficient to Operate, Maintain, or Protect the Network

(U//~~FOUO~~) U.S. Fleet Forces Command and U.S. Pacific Fleet Commanders did not meet Chief of Naval Operations staffing requirements for assigning CANES administrators to ships to ensure that each ship had the necessary number of CANES administrators to operate, maintain, and protect CANES. CANES was designed and fielded to reduce the Navy's cybersecurity attack surface (logical access points that adversaries can use to gain access to a network), mitigate vulnerabilities in a timely manner, and improve system management and detection capabilities. However, the Navy has not sufficiently staffed the ships with trained and certified administrators to operate, maintain, and protect the CANES network. The Chief of Naval Operations requires specific staffing levels for CANES administrators by ship type. [redacted]

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~) [redacted]. The Chief of Naval Personnel and the Commanders of the Naval Education and Training Command, U.S. Fleet Forces, and U.S. Pacific Fleet should implement a plan to staff the required number of CANES administrators per ship established by the Chief of Naval Operations.

## (U//~~FOUO~~) Security Weaknesses May Compromise the CANES Network

(U//~~FOUO~~) [redacted] The DoD requires Components to protect networks and systems using applicable security requirements prescribed in National Institute for Standards and Technology Special Publication 800-53. [redacted].

(U) [redacted]

(U) [redacted]

## (U) Management Comments on the Finding and Our Response

(U) A summary of management comments on the finding and our response are in Appendix D.

## (U) Recommendations, Management Comments, and Our Response

### *(U) Redirected Recommendation*

(U) As a result of management comments from U.S. Pacific Fleet Inspector General, we redirected Recommendation 2 to the Chief of Naval Personnel and the Commander of the Naval Education and Training Command because they have the authority to address Navy staffing and training issues.

### *(U) Recommendation 1*

**(U) We recommend that the Chief of Naval Operations, in coordination with the Commanders of the U.S. Fleet Forces Command and U.S. Pacific Fleet Command and Tactical Networks Program Manager, review the systemic problems identified in this report, and develop and implement a plan of action and milestones to correct network and cybersecurity weaknesses that will:**

a. **~~(C)~~ Mitigate network cyber vulnerabilities.**

b. **~~(C)~~** [redacted]

c. **~~(C)~~** [redacted]

d. **~~(C)~~** [redacted]

e. **~~(C)~~ Account for Consolidated Afloat Networks and Enterprise Services-connected devices.**

f. **~~(C)~~** [redacted]

### *(U) Management Comments Required*

(U) The Chief of Naval Operations did not respond to the recommendation; therefore, the recommendation is unresolved. We request that the Chief of Naval Operations provide comments on the final report.

### *(U) PMW 160 Comments*

(U//~~FOUO~~) Although not required to comment, the Program Executive Officer, Command, Control, Communication, Computers, and Intelligence, responding for PMW 160, stated that the Program Executive Officer and PMW 160 would work with all stakeholders across the enterprise to address the recommendations in this report. In addition, the Program Executive Officer stated that the PMW 160 would also work across the enterprise to address non-cybersecurity problems, such as staffing, that affect the CANES program.

### *(U) U.S. Pacific Fleet Comments*

(U) Although not required to comment, the U.S. Pacific Fleet Inspector General, responding for the U.S. Pacific Fleet Commander, stated that the U.S. Pacific Fleet would support the development and execution of a plan of action and milestones to address the problems and reasons for the problems identified in this report, such as staffing, training, and sustained operations tempo.

### *(U) Our Response*

(U) We look forward to the Program Executive Officer, PMW 160, and U.S. Pacific Fleet Command correcting problems that will protect the CANES network and for their commitment to correct the problems identified in this report enterprise-wide.

## *(U) Recommendation 2*

**(U/~~FOUO~~) We recommend that the Chief of Naval Personnel and the Commander of the Naval Education and Training Command, in coordination with the Commanders of the U.S. Fleet Forces Command and U.S. Pacific Fleet Command, implement a plan to staff the required number of Consolidated Afloat Networks and Enterprise Services administrators per ship established by the Chief of Naval Operations.**

## *(U) Recommendation 3*

**(U) We recommend that the U.S. Ship *Abraham Lincoln*, U.S. Ship *Ronald Reagan*, U.S. Ship *Ramage*, and U.S. Ship *Russell* Commanding Officers, in coordination with the ships' Combat Systems Officers:**

**a.** ~~(S)~~ [redacted]

### *(U) USS Ronald Reagan Comments*

~~(S)~~ The USS *Ronald Reagan* Commanding Officer agreed, [redacted]

### *(U) Our Response*

~~(S)~~ Comments from the Commanding Officer addressed all specifics of the recommendation; therefore, the recommendation is resolved. [redacted]

### *(U) USS Ramage Comments*

~~(S)~~ The Commodore for Destroyer Squadron Two Eight, responding for the USS *Ramage* Commanding Officer, agreed, [redacted]

### *(U) Our Response*

~~(S)~~ Comments from the Commodore addressed all specifics of the recommendation; therefore, the recommendation is resolved. [redacted]

### *(U) USS Russell Comments*

~~(S)~~ The USS *Russell* Commanding Officer agreed, [redacted]

### *(U) Our Response*

~~(S)~~ Comments from the Commanding Officer addressed all specifics of the recommendation; therefore, the recommendation is resolved. [redacted]

### *(U) Management Comments Required*

(U) The USS *Abraham Lincoln* Commanding Officer did not respond to the recommendation; therefore, the recommendation is unresolved. We request that the Commanding Officer provide comments on the final report.

**b. (U) Revise and implement existing inventory procedures to require all ship personnel to request Consolidated Afloat Networks and Enterprise Services' administrator approval before relocating devices and perform monthly reviews to identify the location of all network devices.**

### *(U) USS Ronald Reagan Comments*

(U) The USS *Ronald Reagan* Commanding Officer agreed, stating that officials updated procedures in November 2018, conducted ship-wide training on information systems inventory procedures between August and December 2018, completed a full inventory of network equipment between November 2018 and January 2019, and issued equipment custody cards to appropriate ship personnel.

### *(U) Our Response*

(U) Comments from the Commanding Officer partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. The Commanding Officer did not state whether officials would require personnel to obtain CANES administrator approval before relocating devices and conduct monthly inventories of CANES network devices. We request that the Commanding Officer provide comments on the final report to clarify whether officials implemented procedures requiring CANES administrator approval before relocating devices and monthly inventories of all network devices.

### *(U) USS Ramage* Comments

(U) The Commodore for Destroyer Squadron Two Eight, responding for the USS *Ramage* Commanding Officer, agreed, stating that officials already conducted monthly inventories, but they added spot checks by the Communications Officer to that monthly process. In addition, the Commodore stated that USS *Ramage* officials implemented new training requirements for staff as part of the command indoctrination program. Furthermore, the Commodore stated that USS *Ramage* officials were updating their access control process to establish requirements for moving equipment.

### *(U) Our Response*

(U) Comments from the Commodore addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain signed procedures requiring monthly inventories and periodic spot checks by the Communications Officer, the updated user access request package showing responsibilities for relocating devices is addressed, copies of the January and February 2019 inventory reports, and documentation showing that responsibilities for relocating devices is included in the updated command indoctrination program.

### *(U) USS Russell Comments*

(U) The USS *Russell* Commanding Officer agreed, stating that officials began using an accountability form that requires users who are issued relocatable devices to obtain system administrator approval before moving the devices. In addition, the Commanding Officer stated that the CANES administrators conducted monthly inventories of CANES-connected devices.

## (U) Our Response

(U) Comments from the Commanding Officer addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain an example of the user accountability form, signed procedures requiring monthly inventories of all CANES-connected devices, and copies of the January and February 2019 inventory reports.

## (U) Management Comments Required

(U) The USS *Abraham Lincoln* Commanding Officer did not respond to the recommendation; therefore, the recommendation is unresolved. We request that the Commanding Officer provide comments on the final report.

**c.** ~~(C)~~ [redacted]

## (U) USS Ronald Reagan Comments

(U) The USS *Ronald Reagan* Commanding Officer agreed, [redacted]

## (U) Our Response

(U) Comments from the Commanding Officer addressed all specifics of the recommendation; therefore, the recommendation is resolved. [redacted]

## (U) USS Ramage Comments

~~(C)~~ The Commodore for Destroyer Squadron Two Eight, responding for the USS *Ramage* Commanding Officer, agreed with the recommendation, [redacted]

### *(U) Our Response*

(U) Comments from the Commanding Officer addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain documentation [redacted]

### *(U) USS Russell Comments*

~~(C)~~ The USS *Russell* Commanding Officer agreed, [redacted]

### *(U) Our Response*

(U) Comments from the Commanding Officer addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain documentation [redacted]

### *(U) Management Comments Required*

(U) The USS *Abraham Lincoln* Commanding Officer did not respond to the recommendation; therefore, the recommendation is unresolved. We request that the Commanding Officer provide comments on the final report.

**d. (U) Review and reconcile whether all personnel assigned to each ship have completed Operations Security training and cyber awareness training, and require personnel who have not completed the training to immediately complete the annual security-related training.**

### *(U) USS Ronald Reagan Comments*

(U) The USS *Ronald Reagan* Commanding Officer agreed, stating that officials reviewed the ship's security-related training programs in November 2018 and determined that existing processes required ship personnel to complete monthly topic-specific Operations Security and cyber awareness trainings as part of the command indoctrination program. However, the Commanding Officer stated that the USS *Ronald Reagan* added a general Operations Security training program to its command indoctrination program. The Commanding Officer also stated that, as of February 2019, approximately 95 percent and 91 percent of ship personnel completed Operations Security and cyber awareness training, respectively, with a plan for remaining ship personnel to complete both FY 2019 training requirements by March 15, 2019.

## *(U) Our Response*

(U) Comments from the Commanding Officer addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain documentation, such as training completion reports from the Fleet Management and Planning System, showing all users completed Operations Security and cyber awareness trainings for FY 2019. We also need signed procedures to show that the additional Operations Security training was added to the command indoctrination program.

## *(U) USS Ramage Comments*

(U) The Commodore for Destroyer Squadron Two Eight, responding for the USS *Ramage* Commanding Officer, agreed, stating that officials tracked the completion of information assurance training and disabled accounts if users did not complete required information assurance training. The Commodore stated that USS *Ramage* officials temporarily reactivated user accounts for a 24-hour period to allow users to complete training if they failed to complete the training when required.

## *(U) Our Response*

(U) Comments from the Commodore partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. Although the Commodore stated that information assurance training completion was tracked, she did not state whether USS *Ramage* officials tracked the completion of Operations Security training, which is another required training. We request that the Commanding Officer provide comments on the final report to clarify whether USS *Ramage* officials tracked the completion of Operations Security training as a condition for obtaining and maintaining network access.

## *(U) USS Russell Comments*

(U) The USS *Russell* Commanding Officer agreed, stating that all personnel with access to the network completed security-related training on September 30, 2018.
The Commanding Officer stated that officials implemented a plan to complete the same training requirements for FY 2019 by March 31, 2019, and would require all new personnel assigned to the ship to complete security related training requirements within 48 hours of receiving network access.

### (U) Our Response

(U) Comments from the Commanding Officer addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we obtain documentation, such as training completion reports from the Fleet Management and Planning System, showing all users completed Operations Security and cyber awareness training for FY 2019. We also need a copy of signed procedures requiring new users to complete security-related training within 48 hours of obtaining network access and documentation that shows the new users received the required training.

### (U) Management Comments Required

(U) The USS *Abraham Lincoln* Commanding Officer did not respond to the recommendation; therefore, the recommendation is unresolved. We request that the Commanding Officer provide comments on the final report.

**e.** ~~(S)~~ [redacted]

### (U) USS Ronald Reagan Comments

~~(S)~~ The USS *Ronald Reagan* Commanding Officer agreed, [redacted]

### (U) Our Response

~~(S)~~ Comments from the Commanding Officer addressed all specifics of the recommendation; therefore, the recommendation is resolved. [redacted]

### (U) USS Ramage Comments

~~(S)~~ The Commodore for Destroyer Squadron Two Eight, responding for the USS *Ramage* Commanding Officer, agreed, [redacted]

### *(U) Our Response*

~~(S)~~ Comments from the Commodore addressed all specifics of the recommendation; therefore, the recommendation is resolved. [redacted]

### *(U) USS Russell Comments*

~~(S)~~ The USS *Russell* Commanding Officer agreed, [redacted]

### *(U) Our Response*

~~(S)~~ Comments from the Commanding Officer addressed all specifics of the recommendation; therefore, the recommendation is resolved. [redacted]

### *(U) Management Comments Required*

(U) The USS *Abraham Lincoln* Commanding Officer did not respond to the recommendation; therefore, the recommendation is unresolved. We request that the Commanding Officer provide comments on the final report.

## *(U) Recommendation 4*

**(U//~~FOUO~~) We recommend that the U.S. Ship *Ronald Reagan*, U.S. Ship *Ramage*, and U.S. Ship *Russell* Commanding Officers, in coordination with the ships' Combat Systems Officers,** [redacted]**.**

### (U) USS Ronald Reagan Comments

(U//~~FOUO~~) The USS *Ronald Reagan* Commanding Officer agreed, [redacted]

### (U) Our Response

(U//~~FOUO~~) Comments from the Commanding Officer partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. The Commanding Officer did not address whether officials [redacted]

### (U) USS Ramage Comments

(U//~~FOUO~~) The Commodore for Destroyer Squadron Two Eight, responding for the USS *Ramage*, agreed, [redacted]

### (U) Our Response

(U//~~FOUO~~) Comments from the Commodore partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. [redacted]

### (U) USS Russell Comments

(U//~~FOUO~~) The USS *Russell* Commanding Officer agreed, [redacted]

### *(U) Our Response*

(U//~~FOUO~~) Comments from the Commanding Officer partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. [redacted]

## *(U) Recommendation 5*

**(U) We recommend that the Chief of Naval Operations reissue guidance to require all Navy personnel to complete Operations Security training annually to ensure that users are aware of and understand their responsibilities for safeguarding sensitive and classified information.**

### *(U) Management Comments Required*

(U) The Chief of Naval Operations did not provide comments on the recommendation; therefore, the recommendation is unresolved. We request that the Chief of Naval Operations provide comments on the final report.

## *(U) Recommendation 6*

**~~(S)~~ We recommend that the Commander of Naval Network Warfare Command, in coordination with the U.S. Ship *Abraham Lincoln*, U.S. Ship *Ronald Reagan*, U.S. Ship *Ramage*, and U.S. Ship *Russell* Commanding Officers and the ships' Combat Systems Officers,** [redacted]

### *(U) NETWARCOM Comments*

~~(S)~~ The NETWARCOM Commanding Officer agreed, [redacted]

### *(U) Our Response*

~~(S)~~ Comments from the Commanding Officer did not address the specifics of the recommendation; therefore, the recommendation is unresolved. [redacted]

~~(S)~~ [redacted]

## (U) USS Ronald Reagan Comments

~~(S)~~ Although not required to comment, the USS *Ronald Reagan* Commanding Officer stated [redacted]

## (U) Our Response

~~(S)~~ We appreciate the Commanding Officer taking actions based on our recommendation. [redacted]

## (U) USS Ramage Comments

~~(S)~~ Although not required to comment, the Commodore for Destroyer Squadron Two Eight, responding on behalf of the USS *Ramage* Commanding Officer, stated that [redacted]

## (U) Our Response

(U//~~FOUO~~) We appreciate the Commodore taking actions based on our recommendation. The implementation [redacted] will improve the ship's security and crew's safety.

### *(U) USS Russell Comments*

~~(S)~~ Although not required to comment, the USS *Russell* Commanding stated that [redacted]

### *(U) Our Response*

(U//~~FOUO~~) We appreciate the Commanding Officer taking actions based on our recommendation. The Commanding Officer implementing [redacted] supports a more secure working environment.

## *(U) Recommendation 7*

**(U//~~FOUO~~) We recommend that the Commander of the Naval Network Warfare Command** [redacted]

### *(U) NETWARCOM Comments*

(U//~~FOUO~~) The NETWARCOM Commanding Officer agreed, stating that the Information Assurance and Cybersecurity Program Office, PMW 130, held regularly scheduled Configuration Control Board meetings and issued configured standards for CANES ships using Fleet Advisory Messages. The Commanding Officer also stated that NETWARCOM regularly issued compliance reports Navy-wide.

### *(U) Our Response*

(U//~~FOUO~~) Comments from the Commanding Officer did not address the specifics of the recommendation; therefore, the recommendation is unresolved. [redacted]

## *(U) Recommendation 8*

**(U) We recommend that the Tactical Networks Program Manager:**

**a.** ~~(S)~~ [redacted]

### *(U) PMW 160 Comments*

(U//~~FOUO~~) The Program Executive Officer, Command, Control, Communication, Computers, and Intelligence, responding for PMW 160, agreed, [redacted]

### *(U) Our Response*

(U//~~FOUO~~) Comments from the Program Executive Officer partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. [redacted]

**b.** ~~(S)~~ [redacted]

### *(U) PMW 160 Comments*

(U//~~FOUO~~) The Program Executive Officer, Command, Control, Communication, Computers, and Intelligence, responding for PMW 160, agreed, [redacted]. In addition, the Program Executive Officer stated that the PMW 160 continued to upgrade CANES based on formal test results, operational security events, and certification and accreditation

(U//~~FOUO~~) requirements. Furthermore, the Program Executive Officer stated that the CANES engineering and acquisition strategy required hardware and software reviews on a 4 year cycle.

## *(U) Our Response*

(U//~~FOUO)~~ Comments from the Program Executive Officer partially addressed the specifics of the recommendation; therefore, the recommendations is unresolved. We agree a structured process is needed to acquire and upgrade hardware and software in a constantly changing cybersecurity environment. However, the Program Executive Officer did not address [redacted]. We request that the PMW 160 Program Manager provide comments on the final report that explains and provides documentation that shows the documented planned or implemented actions to mitigate the risk of [redacted]

# (U) Appendix A

## (U) Scope and Methodology

(U) We conducted this performance audit from January 2018 through January 2019 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 interviewed officials from the Director, Operational Test and Evaluation to discuss their previous and ongoing operational evaluations of CANES. In addition, we interviewed officials from SPAWAR, PMW 160, and the Information Assurance and Cyber Security Program Office to discuss their plans and processes for acquiring, implementing, and sustaining CANES. We also interviewed officials from the Navy's Network Operations Centers, Naval Information Forces, and Navy Cyber Defense Operations Command to identify how they monitor afloat network security and train and equip personnel who operate, maintain, and protect CANES. In addition, we attended the Fleet Stakeholder Working Group in March 2018 to obtain information on the CANES network and identify concerns the stakeholders had with CANES operations and security.

(U) We reviewed Federal, DoD, and Navy cybersecurity policies and guidance, a U.S. Cyber Command tasking order, and the Naval Information Forces HBSS concept of operations to identify network security controls that the Navy was required to implement to protect the CANES network. We also reviewed manpower studies, CANES architecture diagrams, network vulnerability scan results, configuration settings, audit logs, and access request forms to assess security risks and test the suitability of implemented network security controls.

(U) We used the CANES implementation plan provided by the PMW 160 to determine the universe of ships with CANES. We randomly selected 4 of the 52 Navy ships that had the CANES network to visit within the scope of this audit. We visited the following ships.

- (U) USS *Abraham Lincoln* and USS *Ramage* in Norfolk, Virginia
- (U) USS *Ronald Reagan* deployed in the Philippine Sea
- (U) USS *Russell* in San Diego, California

(U) For the first visit, we filtered the universe by ships that were based (home port) in Norfolk, Virginia, and were in port between April 23, 2018, and May 11, 2018.[32] For the remaining three ship visits, we separated the universe by ships with a home port in the continental United States and those with a home port outside the continental United States. After selecting the first ship from each sample, we used WebSked (the Navy's official ship scheduling system) to determine the ships' availability.

(U) We met with CANES administrators on the USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell* to determine their roles and responsibilities for operating, maintaining, and protecting CANES. We tested the effectiveness of security safeguards related to:

- (U) boundary defense;
- (U) administering and managing network access;
- (U) audit logging;
- (U) vulnerability management;
- (U) connected device management;
- (U) malware protection; and
- (U) annual Operational Security and cyber awareness training.

(U) For administering and managing network access, connected device management, and annual operational security and cyber awareness training, we performed control tests.[33] For the control tests, we met with the DoD OIG Quantitative Methods Division to discuss our sampling methodology. Based on our meeting, we applied the following decision rules.

- (U) If there were no errors in the sample, then the control passed.
- (U) If there were one or more errors or documentation could not be provided, then the control failed.

(U) To test security safeguards related to boundary defense, we reviewed configurations for security devices, such as firewalls, routers, and switches, within each security domain against Defense Information Systems Agency Security Technical Implementation Guide requirements.

[32] (U) We conducted a random sample of the universe to reduce bias during sample selection.

[33] (U) Council of the Inspector General on Integrity and Efficiency, "Journal of Public Inquiry," Fall/Winter 2012-2013.

(U) To test security safeguards related to administering and managing CANES access, we developed samples for each ship visited to determine whether access request forms were properly completed and included appropriate justification as a condition for obtaining CANES network access. We verified whether users, supervisors, security managers, and Information Assurance Managers approved and signed each request; users completed annual operational security and cyber awareness training; and the forms included justification for access that aligned to their assigned duties. We also determined whether CANES administrators disabled or removed inactive accounts by comparing a list of active user accounts provided by the CANES administrators to a separate list of personnel who had left the ship provided by the ships' administrative department. Table 3 identifies the number of NIPRNet and SIPRNet users and sample size, by ship, and the results of the access control tests.

*(U) Table 3. CANES Access* [redacted] *on the USS Abraham Lincoln, USS Ronald Reagan, USS Ramage, and USS Russell*

Navy (b)(1)(1.7e)

[redacted]

(U) *Not Tested if the access request form was not provided.

(U) Source: The DoD OIG.

(U) To test security safeguards related to audit logging, we obtained and reviewed standard operating procedures and interviewed CANES administrators to determine their processes for identifying unauthorized access and unusual or malicious activities, auditable events that were logged, and any limitations preventing them from reviewing audit logs.

(U) To test security safeguards related to managing vulnerabilities, we obtained vulnerability scans conducted by the CANES administrators from April 2018 through July 2018 aboard each of the four ships visited. We reviewed the reports and reported on only unmitigated CAT I vulnerabilities because they presented the highest risk to each ship.

(U) To test security safeguards related to managing connected devices and protecting against malware, we developed samples for each ship visited to determine whether CANES administrators configured devices to restrict write privileges, regularly identified devices connected to the CANES network, and installed and updated [redacted]. We observed CANES administrators log into each selected device and obtain security configuration and [redacted] software data for each device included in the sample. We reviewed the following based on random samples:

- (U) 44 of 1,124 NIPRNet-connected and 32 of 96 SIPRNet-connected devices as well as 33 of 112 SIPRNet servers on the USS *Abraham Lincoln*;
- (U) 44 of 1,010 NIPRNet-connected and 41 of 253 SIPRNet-connected devices as well as 17 of 30 NIPRNet servers, 33 of 142 SIPRNet servers, and 44 NIPRNet-connected embarkable assets on the USS *Ronald Reagan*;
- (U) 36 of 180 NIPRNet-connected and 33 of 114 SIPRNet-connected devices on the USS *Ramage*; and
- (U) 36 of 176 NIPRNet-connected devices on the USS *Russell*.

## (U) Use of Computer-Processed Data

(U) We used computer-processed data from the CANES Active Directory, the Vulnerability Remediation Asset Manager, and hypertext markup language (html) printouts from selected devices that the Navy converted to Adobe Acrobat and Microsoft Word files.

(U//~~FOUO~~) We obtained and analyzed NIPRNet and SIPRNet data from Active Directory to determine the universe of USS *Abraham Lincoln*, USS *Ronald Reagan*, USS *Ramage*, and USS *Russell* user accounts to test the appropriateness of user access and the completion of annual security training. To assess the reliability of the data, we compared the universe of user accounts to a list of users who had left each ship within 6 months and found discrepancies with the data. Although we identified discrepancies

(U//~~FOUO~~) with the data, we determined that the data were sufficiently reliable to test whether a user's justification for access to the CANES network had been approved and the user completed required training as a condition of access.

(U//~~FOUO~~) We obtained a list of current devices for the USS *Ramage* from Active Directory. We used the data to select samples of devices for testing write privileges and antivirus. To test the reliability of the data, we physically inspected each device in our sample. We identified discrepancies with the sample of devices and determined that the data was not reliable as discussed in the Finding.

(U) We analyzed Assured Compliance Assessment Solution vulnerability scans from the Vulnerability Remediation Asset Manager. We used the data to determine whether the ships managed CAT I vulnerabilities. Assured Compliance Assessment Solution is a DoD tool managed by Defense Information Systems Agency. In addition, we interviewed the Information Assurance and Cyber Security Program Office about the reliability of the Vulnerability Remediation Asset Manager. We determined that these documents were sufficiently reliable for the purpose of this report.

## (U) Use of Technical Assistance

(U) The DoD OIG Quantitative Methods Division provided assistance in developing and selecting samples of CANES ships, network devices, and user accounts.

## (U) Prior Coverage

(U) No prior coverage has been conducted on the Navy's CANES network during the last 5 years.

# (U) Appendix B

## (U) Roles and Responsibilities

(U) Several Navy commands are responsible for operating, maintaining, and protecting CANES.

### *(U) SPAWAR*

(U) SPAWAR identifies, develops, delivers, and sustains information warfighting capabilities that support naval, joint, coalition, and other national missions. SPAWAR assists PMW 160 in developing, sustaining, and installing CANES by providing contracting, engineering, and logistical expertise.

### *(U) PMW 160*

(U) PMW 160 acquires and sustains hardware and software to support the CANES infrastructure. PMW 160 provides cyber resiliency for the CANES network by integrating emerging technologies and ensuring end-to-end network alignment to support warfighter use. PMW 160 delivers integrated wide-area, local network, and computing and data systems afloat that support geographically dispersed Navy, joint, and coalition networks.

### *(U) Information Assurance and Cyber Security Program Office*

(U) The Information Assurance and Cyber Security Program Office plans, manages, and executes program resources to protect Navy and joint information, telecommunications, and information systems from cyberattacks. The Program Office acquires and sustains cybersecurity products and services to ensure strong authentication, data integrity, confidentiality, non-repudiation, and availability of network resources and information. The Program Office provides cybersecurity products such as cross-domain solutions, cyber defense toolkits, and a vulnerability remediation asset manager to support CANES network security operations.[34]

### *(U) Navy Cyber Defense Operations Command*

(U) The Navy Cyber Defense Operation Command coordinates, monitors, and oversees the defense of Navy computer networks and systems, including telecommunications and computer network defenses used by CANES and other Navy networks.

[34] (U) Cross-domain solutions provide the ability to manually or automatically access or transfer information between different security domains. Cyber defense toolkits are used by Navy network defenders to identify network intrusions and collect network audit logs.

## *(U) Type Commands*

(U) Naval Information Forces, Naval Surface Forces Command, and Naval Air Forces Command staff, train, and equip the fleet. Naval Information Forces provides naval and joint operational commanders with Information Warfare forces, including CANES administrators, to execute missions in support of U.S. interests worldwide. Naval Surface Forces Command ensures surface ships, including cruisers, destroyers, frigates, amphibious assault ships, and logistics and fleet support ships, meet readiness requirements while Naval Air Forces Command ensures aircraft carriers and air squadrons meet readiness requirements, including those related to managing and protecting afloat networks such as CANES.

## *(U) NETWARCOM*

(U) NETWARCOM executes tactical-level command and control to direct, operate, maintain, and protect Navy communications and network systems. NETWARCOM manages the Host Based Security System for ships with CANES.

## *(U) CANES Administrators*

(U) The CANES administrators maintain and protect CANES on a daily basis by reviewing network-generated logs; managing network access; installing, configuring, and monitoring security devices; and performing general maintenance and troubleshooting.

## *(U) Navy Network Operations Centers*

(U) The Navy Network Operations Centers provide network management and monitoring, help desk support, user administration, information security assurance, and network access. There are four Network Operations Centers worldwide that ensure ships receive secure, reliable, and seamless access to information and network services.

# (U) Appendix C

## (U) Ships with CANES

(U) PMW 160 documentation shows that it installed CANES aboard 67 ships as of September 2018. The table identifies the ship and installation date. Information is presented based on the CANES hardware and software version installed.

UNCLASSIFIED

| | Ship | CANES Version | CANES Variant | Last Install/Update |
|---|---|---|---|---|
| 1 | USS *Milius* (DDG-69) | HW 1 /<br>SW 1.0.0.3 | Unit Level | January 29, 2014 |
| 2 | USS *Fitzgerald* (DDG-62) | HW 1 /<br>SW 1.0.0.3 | Unit Level | January 30, 2014 |
| 3 | USS *Chafee* (DDG-90) | HW 1 /<br>SW 1.0.0.3 | Unit Level | March 7, 2014 |
| 4 | USS *Porter* (DDG-78) | HW 1 /<br>SW 1.0.0.3 | Unit Level | August 29, 2014 |
| 5 | USS *McFaul* (DDG-74) | HW 1 /<br>SW 1.0.0.3 | Unit Level | September 19, 2014 |
| 6 | USS *Laboon* (DDG-58) | HW 1 /<br>SW 1.0.0.3 | Unit Level | January 2, 2015 |
| 7 | USS *Higgins* (DDG-76) | HW 1 /<br>SW 1.0.0.4 | Unit Level | June 5, 2014 |
| 8 | USS *McCampbell* (DDG-85) | HW 1 /<br>SW 1.0.0.4 | Unit Level | July 29, 2014 |
| 9 | USS *Gonzalez* (DDG-66) | HW 1 /<br>SW 1.0.0.4 | Unit Level | September 11, 2014 |
| 10 | USS *Russell* (DDG-59) | HW 1 /<br>SW 1.0.0.4 | Unit Level | September 12, 2014 |
| 11 | USS *The Sullivans* (DDG-68) | HW 1 /<br>SW 1.0.0.4 | Unit Level | December 19, 2014 |
| 12 | USS *Stout* (DDG-55) | HW 1 /<br>SW 1.0.0.4 | Unit Level | January 5, 2015 |
| 13 | USS *Ramage* (DDG-61) | HW 1 /<br>SW 1.0.0.4 | Unit Level | January 26, 2015 |
| 14 | USS *Curtis Wilbur* (DDG-54) | HW 1 /<br>SW 1.0.0.4 | Unit Level | February 4, 2015 |
| 15 | USS *Decatur* (DDG-73) | HW 1 /<br>SW 1.0.0.4 | Unit Level | April 3, 2015 |
| 16 | USS *Monterey* (CG-61) | HW 1 /<br>SW 1.0.0.4 | Unit Level | May 8, 2015 |
| 17 | USS *San Jacinto* (CG-56) | HW 1 /<br>SW 1.0.0.4 | Unit Level | May 13, 2015 |

**UNCLASSIFIED**

UNCLASSIFIED

| | Ship | CANES Version | CANES Variant | Last Install/Update |
|---|---|---|---|---|
| 18 | USS *Stethem* (DDG-63) | HW 1 / SW 1.0.0.4 | Unit Level | July 3, 2015 |
| 19 | USS *Carter Hall* (LSD-50) | HW 1 / SW 1.0.0.4 | Unit Level | August 21, 2015 |
| 20 | USS *Pinckney* (DDG-91) | HW 1 / SW 1.0.0.4 | Unit Level | November 25, 2015 |
| 21 | USS *Cole* (DDG-67) | HW 1 / SW1.0.0.4 | Unit Level | December 15, 2015 |
| 22 | USS *Comstock* (LSD-45) | HW 1 / SW 1.0.0.4 | Unit Level | January 22, 2016 |
| 23 | USS *John S. McCain* (DDG-56) | HW 1 / SW 1.0.0.4 | Unit Level | April 29, 2016 |
| 24 | USS *Kidd* (DDG-100) | HW 1 / SW 1.0.0.4 | Unit Level | May 6, 2016 |
| 25 | USS *Jason Dunham* (DDG-109) | HW 1 / SW 1.0.0.4 | Unit Level | July 15, 2016 |
| 26 | USS *Oscar Austin* (DDG-79) | HW 1 / SW 1.0.0.4 | Unit Level | July 22, 2016 |
| 27 | USS *Forrest Sherman* (DDG-98) | HW 1 / SW 1.0.0.4 | Unit Level | September 2, 2016 |
| 28 | USS *Mustin* (DDG-89) | HW 1 / SW 1.0.0.4 | Unit Level | September 2, 2016 |
| 29 | USS *Halsey* (DDG-97) | HW 1 / SW 1.0.0.4 | Unit Level | September 8, 2016 |
| 30 | USS *John C. Stennis* (CVN-74) | HW 1 / SW 1.0.0.6 | Force Level | October 17, 2014 |
| 31 | USS *Ronald Reagan* (CVN-76) | HW 1 / SW 1.0.0.6 | Force Level | March 6, 2015 |
| 32 | USS *Bataan* (LHD-5) | HW 1 / SW 1.0.0.6 | Force Level | February 1, 2016 |
| 33 | USS *Carl Vinson* (CVN-70) | HW 1 / SW 1.0.0.6 | Force Level | April 29, 2016 |
| 34 | USS *Iwo Jima* (LHD-7) | HW 1 / SW 1.0.0.6 | Force Level | June 17, 2016 |
| 35 | USS *Nimitz* (CVN-68) | HW 1 / SW 1.0.0.6 | Force Level | November 18, 2016 |
| 36 | USS *Abraham Lincoln* (CVN-72) | HW 1 / SW 1.0.0.6 | Force Level | September 8, 2017 |
| 37 | USS *Wasp* (LHD-1) | HW 1 / SW 1.0.0.9 | Force Level | July 6, 2017 |
| 38 | USS *Momsen* (DDG-92) | HW 1 / SW 1.0.0.9 | Unit Level | September 5, 2017 |
| 39 | USS *Dwight D. Eisenhower* (CVN-69) | HW 1 / SW 1.0.0.9 | Force Level | March 3, 2015 |
| 40 | USS *Mason* (DDG-87) | HW 1 / SW 1.0.0.9 | Unit Level | January 8, 2015 |

**UNCLASSIFIED**

UNCLASSIFIED

| | Ship | CANES Version | CANES Variant | Last Install/Update |
|---|---|---|---|---|
| 41 | USS *Theodore Roosevelt* (CVN-71) | HW 1.1 / SW 1.0.1 | Force Level | January 11, 2017 |
| 42 | USS *Essex* (LHD-2) | HW 1.1 / SW 1.0.1 | Force Level | April 5, 2017 |
| 43 | USS *Harry S. Truman* (CVN-75) | HW 1.1 / SW 1.0.1 | Force Level | August 4, 2017 |
| 44 | USS *Bainbridge* (DDG-96) | HW 1.1 / SW 1.0.1 | Unit Level | March 10, 2017 |
| 45 | USS *Rushmore* (LSD-47) | HW 1.1 / SW 1.0.1 | Unit Level | March 10, 2017 |
| 46 | USS *Farragut* (DDG-99) | HW 1.1 / SW 1.0.1 | Unit Level | May 25, 2017 |
| 47 | USS *Chung-Hoon* (DDG-93) | HW 1.1 / SW 1.0.1 | Unit Level | July 1, 2017 |
| 48 | USS *Gravely* (DDG-107) | HW 1.1 / SW 1.0.1 | Unit Level | July 5, 2017 |
| 49 | USS *Stockdale* (DDG-106) | HW 1.1 / SW 1.0.1 | Unit Level | August 18, 2017 |
| 50 | USS *Oak Hill* (LSD-51) | HW 1.1 / SW 1.0.1 | Unit Level | October 30, 2017 |
| 51 | USS *Paul Hamilton* (DDG-60) | HW 1.1 / SW 1.0.1 | Unit Level | February 8, 2018 |
| 52 | USS *Blue Ridge* (LCC-19) | HW 1.1 / SW 1.2 | Force Level | June 21, 2017 |
| 53 | USS *Mt Whitney* (LCC-20) | HW 1.1 / SW 1.2 | Force Level | September 11, 2017 |
| 54 | USS *New Orleans* (LPD-18) | HW 1.1 / SW 2 | Force Level | July 27, 2018 |
| 55 | USS *Maryland* (SSBN-738) | HW 0 / SW 0 | Submarine | December 15, 2014 |
| 56 | USS *Scranton* (SSN-756) | HW 0 / SW 0 | Submarine | February 24, 2016 |
| 57 | USS *Nevada* (SSBN-733) | HW 0 / SW 0 | Submarine | April 22, 2016 |
| 58 | USS *Nebraska* (SSBN-739) | HW 0 / SW 0 | Submarine | April 28, 2016 |
| 59 | USS *Asheville* (SSN-758) | HW 0 / SW 0 | Submarine | April 26, 2017 |
| 60 | USS *Albany* (SSN-753) | HW 0 / SW 0 | Submarine | August 18, 2017 |
| 61 | USS *Tennessee* (SSBN-734) | HW 1.1 / SW ORT | Submarine | July 13, 2016 |
| 62 | USS *Annapolis* (SSN-760) | HW 1.1 / SW ORT | Submarine | February 22, 2017 |
| 63 | USS *Henry M Jackson* (SSBN-730) | HW 1.1 / SW ORT | Submarine | July 20, 2017 |

UNCLASSIFIED

UNCLASSIFIED

| | Ship | CANES Version | CANES Variant | Last Install/Update |
|---|---|---|---|---|
| 64 | USS *West Virginia* (SSN-736) | HW 1.1 /<br>SW ORT | Submarine | November 17, 2017 |
| 65 | USS *Rhode Island* (SSBN-740) | HW 1.1 /<br>SW ORT | Submarine | November 21, 2017 |
| 66 | USS *Hampton* (SSN-767) | HW 1.1 /<br>SW ORT | Submarine | November 21, 2017 |
| 67 | USS *Montpelier* (SSN-765) | HW 1.1 /<br>SW ORT | Submarine | March 12, 2018 |

**UNCLASSIFIED**

**(U) Legend**
(U) CG – Guided Missile Cruiser
(U) CVN – Multi-purpose Aircraft Carrier
(U) DDG – Guided Missile Destroyer
(U) LCC – Amphibious Command Ship
(U) LHD – Amphibious Assault Ship
(U) HW – Hardware
(U) LPD – Amphibious Transport Dock
(U) LSD – Dock Landing Ship
(U) ORT – Operation Rolling Tide
(U) SSBN – Ballistic Missile Submarine
(U) SSN – Nuclear-powered Attack Submarine
(U) SW – Software

(U) Source: PMW 160.

# (U) Appendix D

## (U) Management Comments on the Finding and Our Response

### *(U) PMW 160 Comments*

(U//~~FOUO~~) The Program Executive Officer, Command, Control, Communication, Computers, and Intelligence, responding for PMW 160, stated that the findings identified in this report are consistent with previous inspections and operational testing performed on the CANES network and the recommendations highlight systemic challenges within the greater Navy enterprise. The Program Executive Officer also stated that the Program Executive Office and PMW 160 are committed to working across the enterprise to address the issues contained in this report.

### *(U) Our Response*

(U//~~FOUO~~) Comments from the Program Executive Officer further demonstrate the need for a comprehensive review of the systematic issues identified in this report across the Fleet, and for the development and implementation of a plan of action and milestones to mitigate cybersecurity weaknesses affecting the CANES network.

### *(U) USS Ronald Reagan Comments*

(U) The USS *Ronald Reagan* Commanding Officer stated that the report was timely and included recommendations that provide the foundational concepts of a sound unit-level cybersecurity program and reinforce the principles of due care and diligence for the ship's cybersecurity workforce. The Commanding Officer also addressed the following systemic CANES program-level security shortfalls observed by USS *Ronald Reagan* officials.

- (U) An evaluation of the CANES maintenance and training programs is needed to ensure that units are properly manned and trained. The Commanding Officer stated that administrators are not sufficiently trained on essential CANES network management tools, such as Cisco network equipment, Virtual Machine software, and Microsoft system engineering, which results in administrators being completely reliant on external support to perform maintenance and security tasks. The Commanding Officer added that a lack of sufficiently trained administrators affects a ship's ability to effectively maintain and operate the ship's combat systems, to include CANES.

- ~~(S)~~ [redacted]
- ~~(S)~~ [redacted]
- ~~(S)~~ [redacted]
- ~~(S)~~ [redacted]

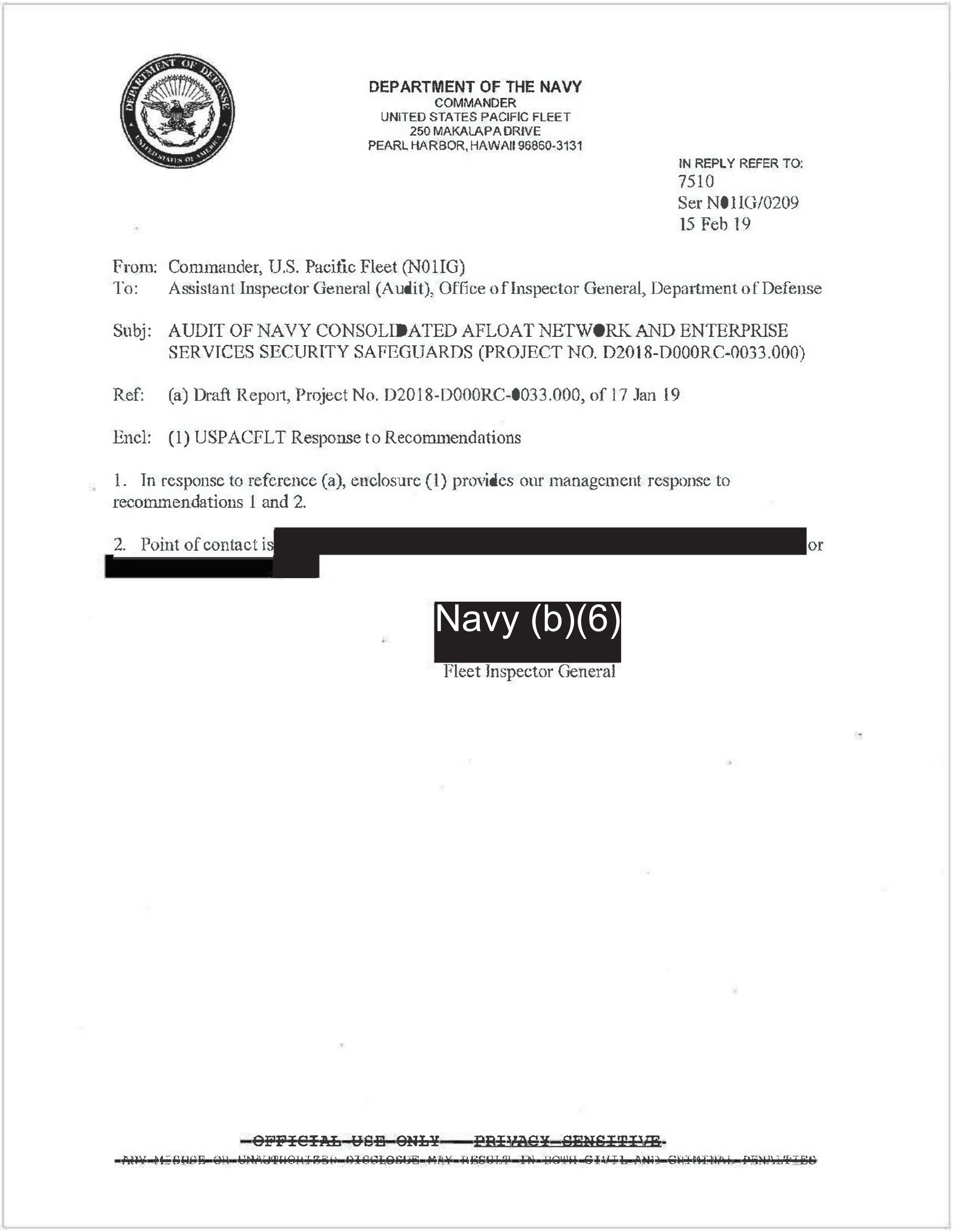
## (U) Our Response

(U//~~FOUO~~) Comments from the USS *Ronald Reagan* Commanding Officer demonstrate the need for a comprehensive review of the CANES program across the Navy relating to security safeguards for protecting the CANES network. Specifically, the Commanding Officer's comments highlighted several key problems regarding protecting and maintaining the CANES network, such as staffing and training of CANES administrators, [redacted].

Additionally, comments from the Commanding Officer demonstrate the need for the Chief of Naval Personnel and the Commander of the Naval Training and Education to implement a plan to staff the required number of trained CANES administrators. The Commanding Officer's comments amplify the concerns we raised in this report and align with the recommendations we made to the Chief of Naval Operations, Chief of Naval Personnel, Commander of the Naval Education and Training Command, Commander of the NETWARCOM, and PMW 160 Program Manager to address the problems enterprise-wide.

# (U) Management Comments

## (U) U.S. Pacific Fleet



DEPARTMENT OF THE NAVY
COMMANDER
UNITED STATES PACIFIC FLEET
250 MAKALAPA DRIVE
PEARL HARBOR, HAWAII 96860-3131

IN REPLY REFER TO:
7510
Ser N01IG/0209
15 Feb 19

From: Commander, U.S. Pacific Fleet (N01IG)
To: Assistant Inspector General (Audit), Office of Inspector General, Department of Defense

Subj: AUDIT OF NAVY CONSOLIDATED AFLOAT NETWORK AND ENTERPRISE SERVICES SECURITY SAFEGUARDS (PROJECT NO. D2018-D000RC-0033.000)

Ref: (a) Draft Report, Project No. D2018-D000RC-0033.000, of 17 Jan 19

Encl: (1) USPACFLT Response to Recommendations

1. In response to reference (a), enclosure (1) provides our management response to recommendations 1 and 2.

2. Point of contact is [redacted] or [redacted]

Navy (b)(6)
Fleet Inspector General

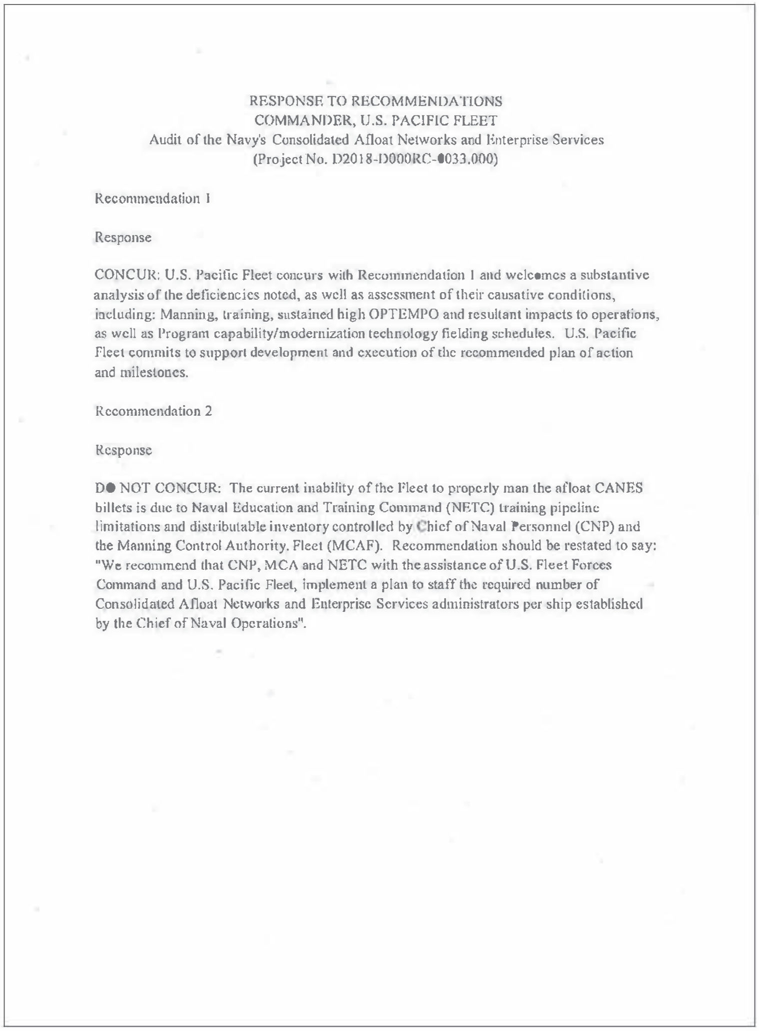
~~OFFICIAL USE ONLY — PRIVACY SENSITIVE~~
~~ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES~~

## (U) U.S. Pacific Fleet (cont'd)

~~FOR OFFICIAL USE ONLY~~

### U.S. Pacific Fleet Commander Comments

**Final Report Reference**



RESPONSE TO RECOMMENDATIONS
COMMANDER, U.S. PACIFIC FLEET
Audit of the Navy's Consolidated Afloat Networks and Enterprise Services
(Project No. D2018-D000RC-0033.000)

Recommendation 1

Response

CONCUR: U.S. Pacific Fleet concurs with Recommendation 1 and welcomes a substantive analysis of the deficiencies noted, as well as assessment of their causative conditions, including: Manning, training, sustained high OPTEMPO and resultant impacts to operations, as well as Program capability/modernization technology fielding schedules. U.S. Pacific Fleet commits to support development and execution of the recommended plan of action and milestones.

Recommendation 2

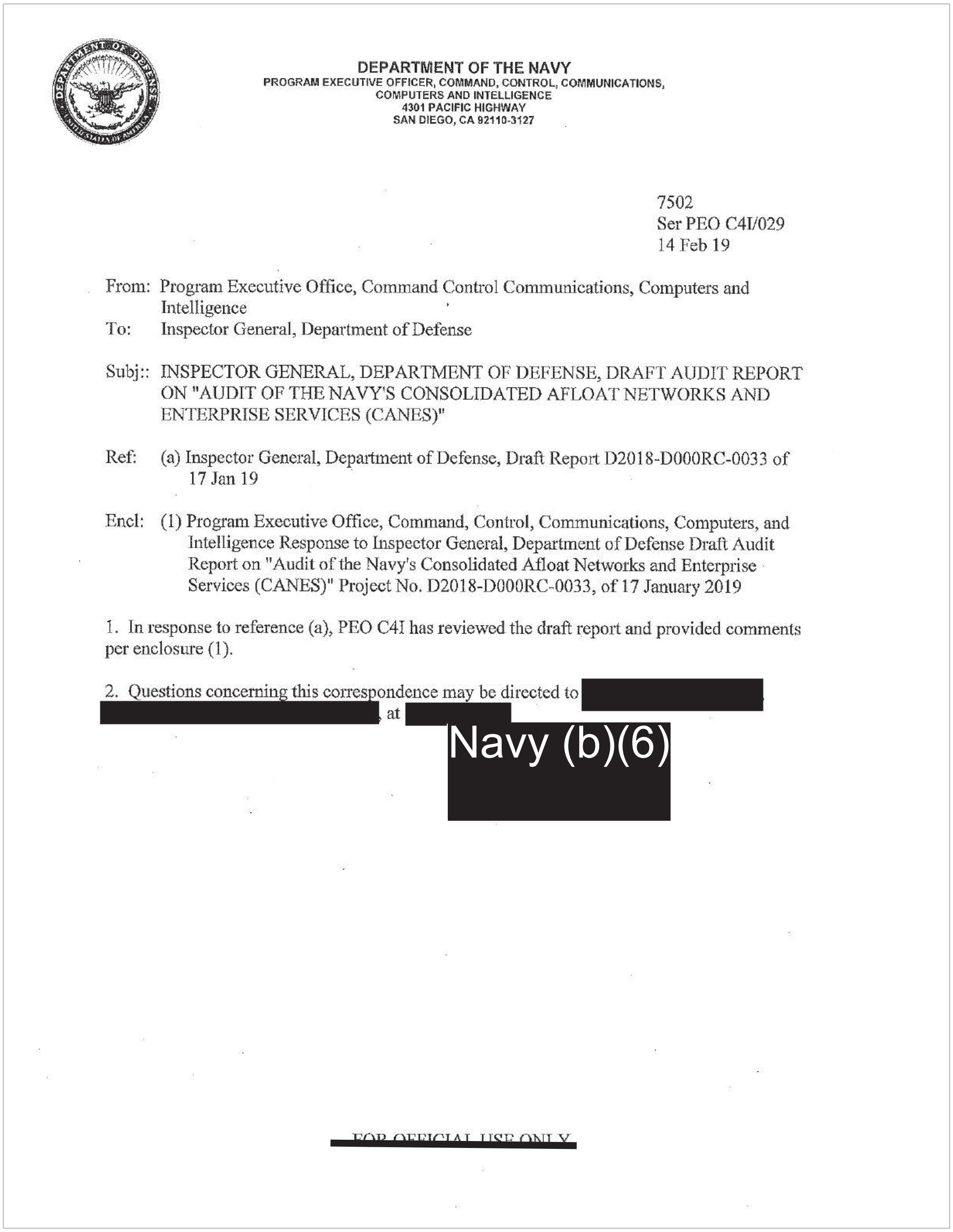
Response

Redirected Recommendation 2

DO NOT CONCUR: The current inability of the Fleet to properly man the afloat CANES billets is due to Naval Education and Training Command (NETC) training pipeline limitations and distributable inventory controlled by Chief of Naval Personnel (CNP) and the Manning Control Authority, Fleet (MCAF). Recommendation should be restated to say: "We recommend that CNP, MCA and NETC with the assistance of U.S. Fleet Forces Command and U.S. Pacific Fleet, implement a plan to staff the required number of Consolidated Afloat Networks and Enterprise Services administrators per ship established by the Chief of Naval Operations".

~~FOR OFFICIAL USE ONLY~~

# (U) Program Executive Officer, Command, Control, Communication, Computers, and Intelligence



DEPARTMENT OF THE NAVY
PROGRAM EXECUTIVE OFFICER, COMMAND, CONTROL, COMMUNICATIONS,
COMPUTERS AND INTELLIGENCE
4301 PACIFIC HIGHWAY
SAN DIEGO, CA 92110-3127

7502
Ser PEO C4I/029
14 Feb 19

From: Program Executive Office, Command Control Communications, Computers and Intelligence
To: Inspector General, Department of Defense

Subj:: INSPECTOR GENERAL, DEPARTMENT OF DEFENSE, DRAFT AUDIT REPORT ON "AUDIT OF THE NAVY'S CONSOLIDATED AFLOAT NETWORKS AND ENTERPRISE SERVICES (CANES)"

Ref: (a) Inspector General, Department of Defense, Draft Report D2018-D000RC-0033 of 17 Jan 19

Encl: (1) Program Executive Office, Command, Control, Communications, Computers, and Intelligence Response to Inspector General, Department of Defense Draft Audit Report on "Audit of the Navy's Consolidated Afloat Networks and Enterprise Services (CANES)" Project No. D2018-D000RC-0033, of 17 January 2019

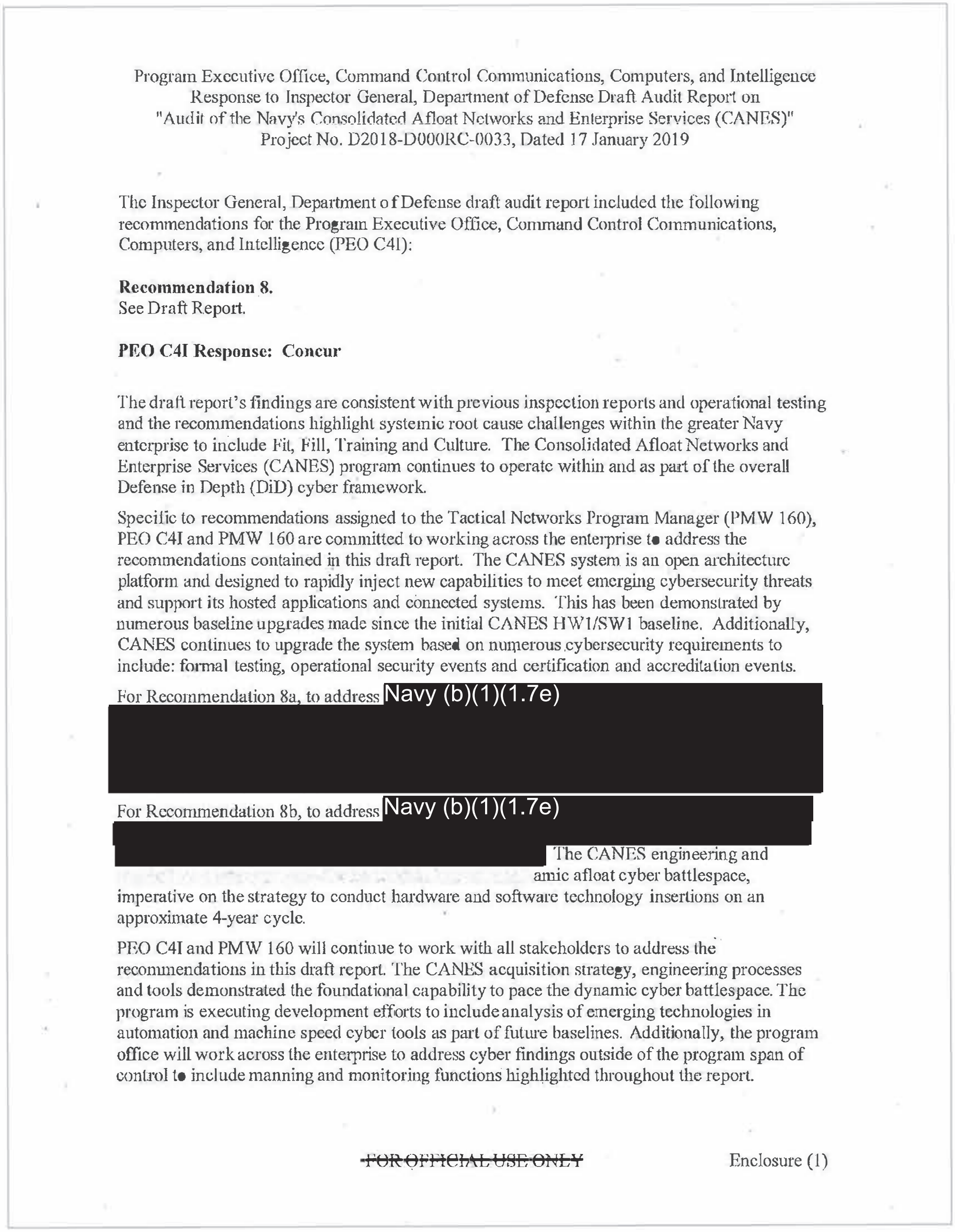
1. In response to reference (a), PEO C4I has reviewed the draft report and provided comments per enclosure (1).

2. Questions concerning this correspondence may be directed to [redacted] [redacted], at [redacted]

Navy (b)(6)

~~FOR OFFICIAL USE ONLY~~

## (U) Program Executive Officer, Command, Control, Communication, Computers, and Intelligence (cont'd)



Program Executive Office, Command Control Communications, Computers, and Intelligence
Response to Inspector General, Department of Defense Draft Audit Report on
"Audit of the Navy's Consolidated Afloat Networks and Enterprise Services (CANES)"
Project No. D2018-D000RC-0033, Dated 17 January 2019

The Inspector General, Department of Defense draft audit report included the following recommendations for the Program Executive Office, Command Control Communications, Computers, and Intelligence (PEO C4I):

**Recommendation 8.**
See Draft Report.

**PEO C4I Response: Concur**

The draft report's findings are consistent with previous inspection reports and operational testing and the recommendations highlight systemic root cause challenges within the greater Navy enterprise to include Fit, Fill, Training and Culture. The Consolidated Afloat Networks and Enterprise Services (CANES) program continues to operate within and as part of the overall Defense in Depth (DiD) cyber framework.

Specific to recommendations assigned to the Tactical Networks Program Manager (PMW 160), PEO C4I and PMW 160 are committed to working across the enterprise to address the recommendations contained in this draft report. The CANES system is an open architecture platform and designed to rapidly inject new capabilities to meet emerging cybersecurity threats and support its hosted applications and connected systems. This has been demonstrated by numerous baseline upgrades made since the initial CANES HW1/SW1 baseline. Additionally, CANES continues to upgrade the system based on numerous cybersecurity requirements to include: formal testing, operational security events and certification and accreditation events.

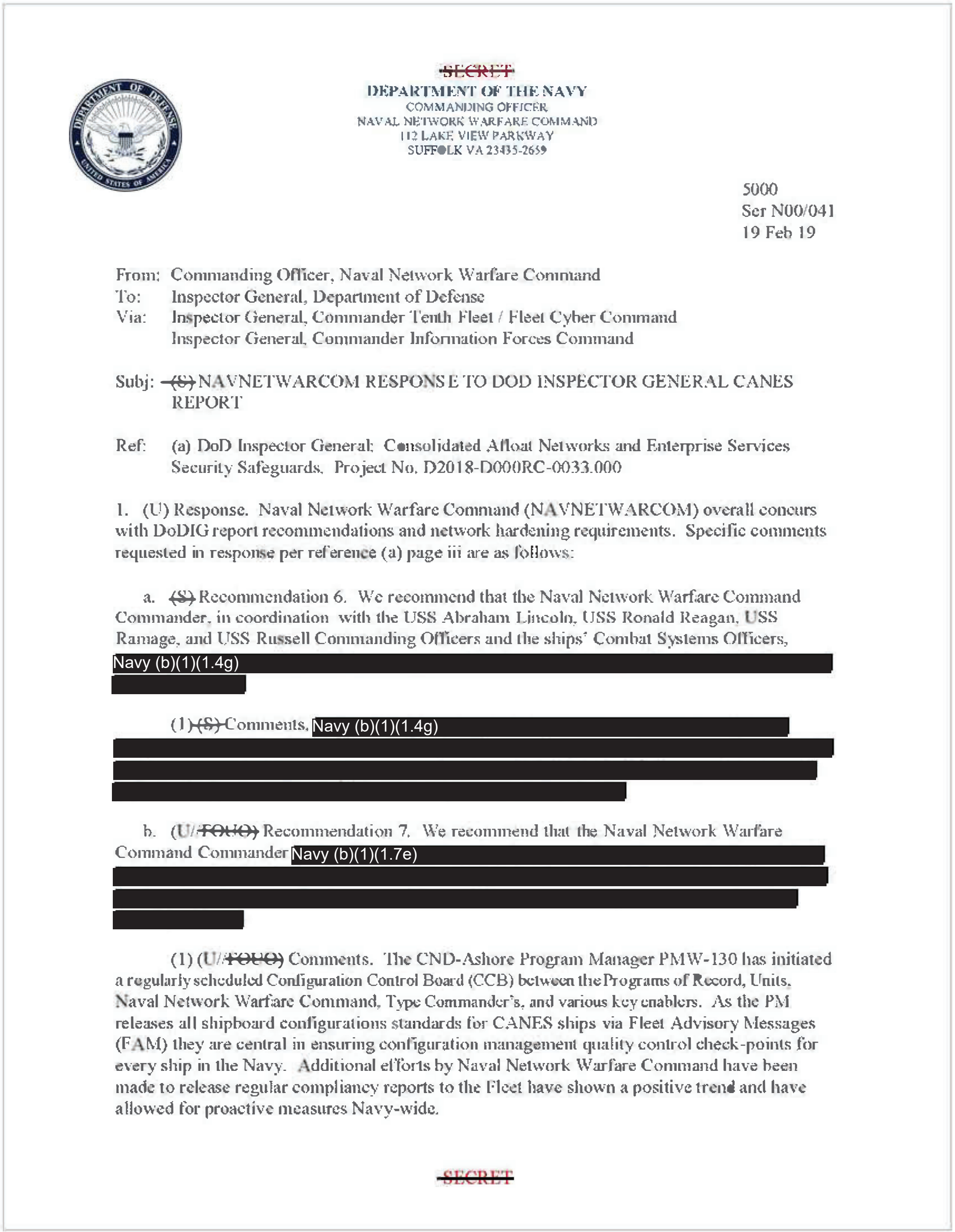
For Recommendation 8a, to address Navy (b)(1)(1.7e)

For Recommendation 8b, to address Navy (b)(1)(1.7e) The CANES engineering and amic afloat cyber battlespace, imperative on the strategy to conduct hardware and software technology insertions on an approximate 4-year cycle.

PEO C4I and PMW 160 will continue to work with all stakeholders to address the recommendations in this draft report. The CANES acquisition strategy, engineering processes and tools demonstrated the foundational capability to pace the dynamic cyber battlespace. The program is executing development efforts to include analysis of emerging technologies in automation and machine speed cyber tools as part of future baselines. Additionally, the program office will work across the enterprise to address cyber findings outside of the program span of control to include manning and monitoring functions highlighted throughout the report.

~~FOR OFFICIAL USE ONLY~~ Enclosure (1)

## (U) Naval Network Warfare Command



~~SECRET~~

DEPARTMENT OF THE NAVY
COMMANDING OFFICER
NAVAL NETWORK WARFARE COMMAND
112 LAKE VIEW PARKWAY
SUFFOLK VA 23435-2659

5000
Ser N00/041
19 Feb 19

From: Commanding Officer, Naval Network Warfare Command
To: Inspector General, Department of Defense
Via: Inspector General, Commander Tenth Fleet / Fleet Cyber Command
Inspector General, Commander Information Forces Command

Subj: ~~(S)~~ NAVNETWARCOM RESPONSE TO DOD INSPECTOR GENERAL CANES REPORT

Ref: (a) DoD Inspector General: Consolidated Afloat Networks and Enterprise Services Security Safeguards. Project No. D2018-D000RC-0033.000

1. (U) Response. Naval Network Warfare Command (NAVNETWARCOM) overall concurs with DoDIG report recommendations and network hardening requirements. Specific comments requested in response per reference (a) page iii are as follows:

a. ~~(S)~~ Recommendation 6. We recommend that the Naval Network Warfare Command Commander, in coordination with the USS Abraham Lincoln, USS Ronald Reagan, USS Ramage, and USS Russell Commanding Officers and the ships' Combat Systems Officers, Navy (b)(1)(1.4g)

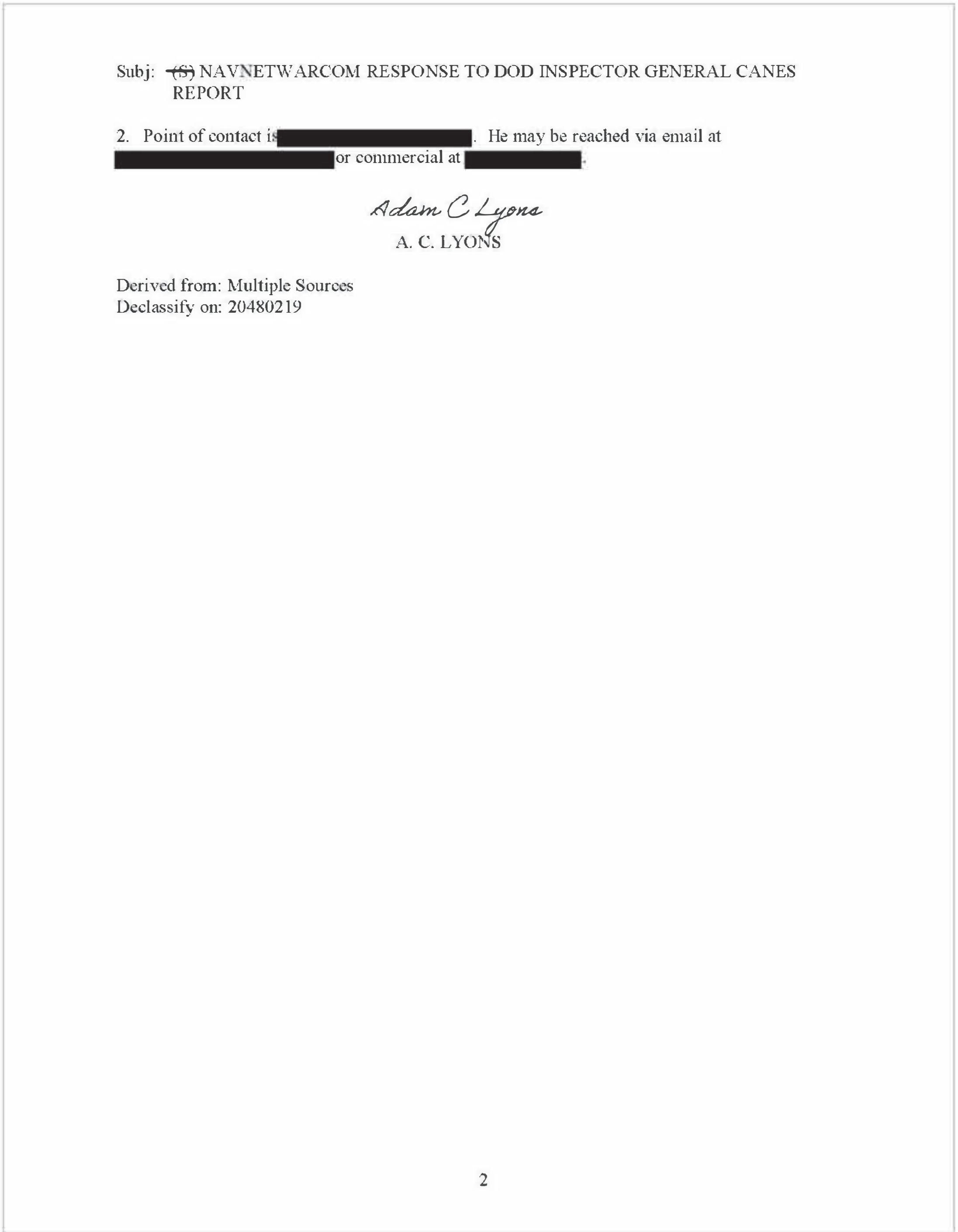
(1) ~~(S)~~ Comments. Navy (b)(1)(1.4g)

b. (U/~~FOUO~~) Recommendation 7. We recommend that the Naval Network Warfare Command Commander Navy (b)(1)(1.7e)

(1) (U/~~FOUO~~) Comments. The CND-Ashore Program Manager PMW-130 has initiated a regularly scheduled Configuration Control Board (CCB) between the Programs of Record, Units, Naval Network Warfare Command, Type Commander's, and various key enablers. As the PM releases all shipboard configurations standards for CANES ships via Fleet Advisory Messages (FAM) they are central in ensuring configuration management quality control check-points for every ship in the Navy. Additional efforts by Naval Network Warfare Command have been made to release regular compliancy reports to the Fleet have shown a positive trend and have allowed for proactive measures Navy-wide.

~~SECRET~~

# (U) Naval Network Warfare Command (cont'd)



Subj: ~~(S)~~ NAVNETWARCOM RESPONSE TO DOD INSPECTOR GENERAL CANES REPORT

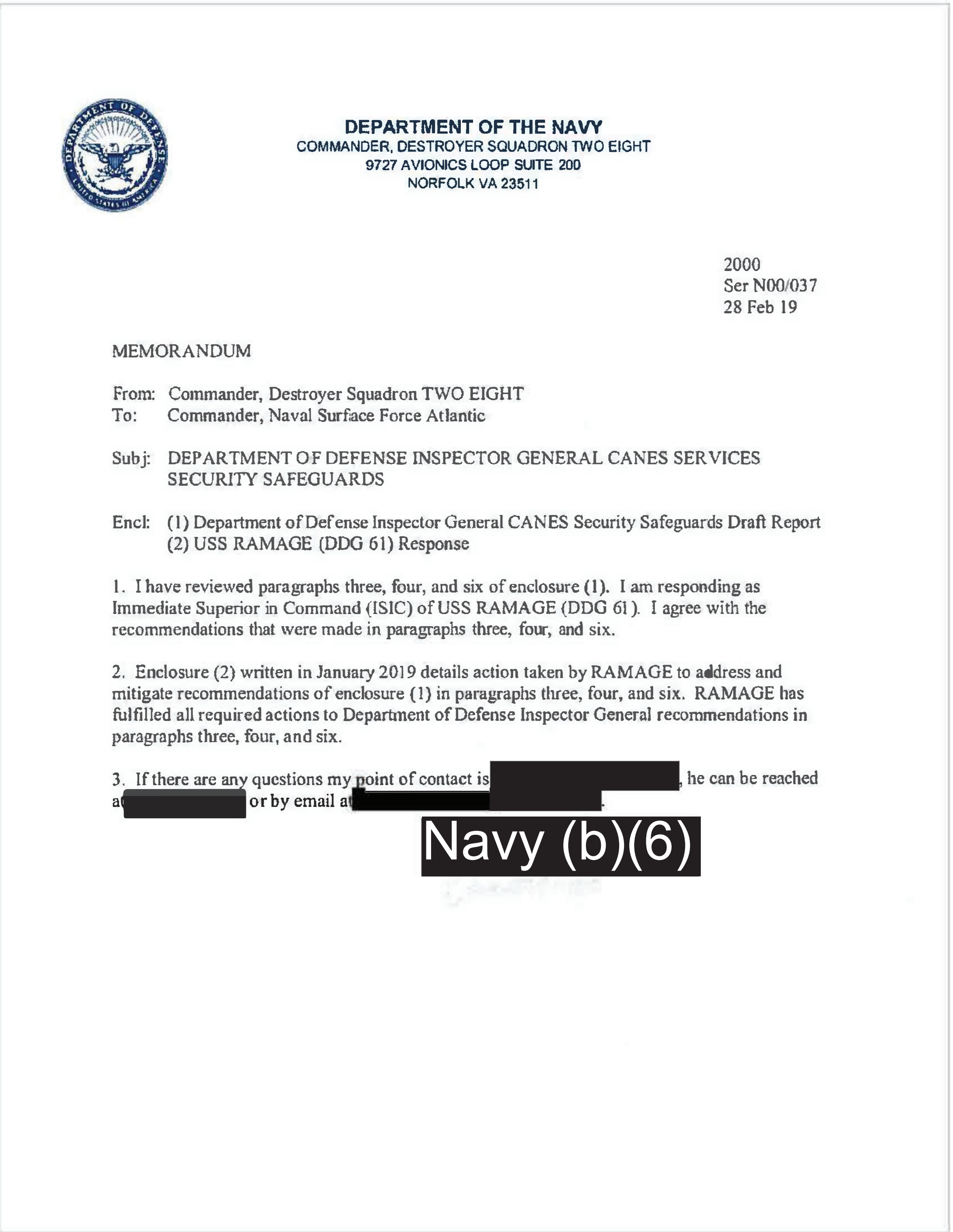
2. Point of contact is [redacted]. He may be reached via email at [redacted] or commercial at [redacted].

Adam C Lyons
A. C. LYONS

Derived from: Multiple Sources
Declassify on: 20480219

2

## (U) Destroyer Squadron Two Eight



DEPARTMENT OF THE NAVY
COMMANDER, DESTROYER SQUADRON TWO EIGHT
9727 AVIONICS LOOP SUITE 200
NORFOLK VA 23511

2000
Ser N00/037
28 Feb 19

MEMORANDUM

From: Commander, Destroyer Squadron TWO EIGHT
To: Commander, Naval Surface Force Atlantic

Subj: DEPARTMENT OF DEFENSE INSPECTOR GENERAL CANES SERVICES SECURITY SAFEGUARDS

Encl: (1) Department of Defense Inspector General CANES Security Safeguards Draft Report
(2) USS RAMAGE (DDG 61) Response

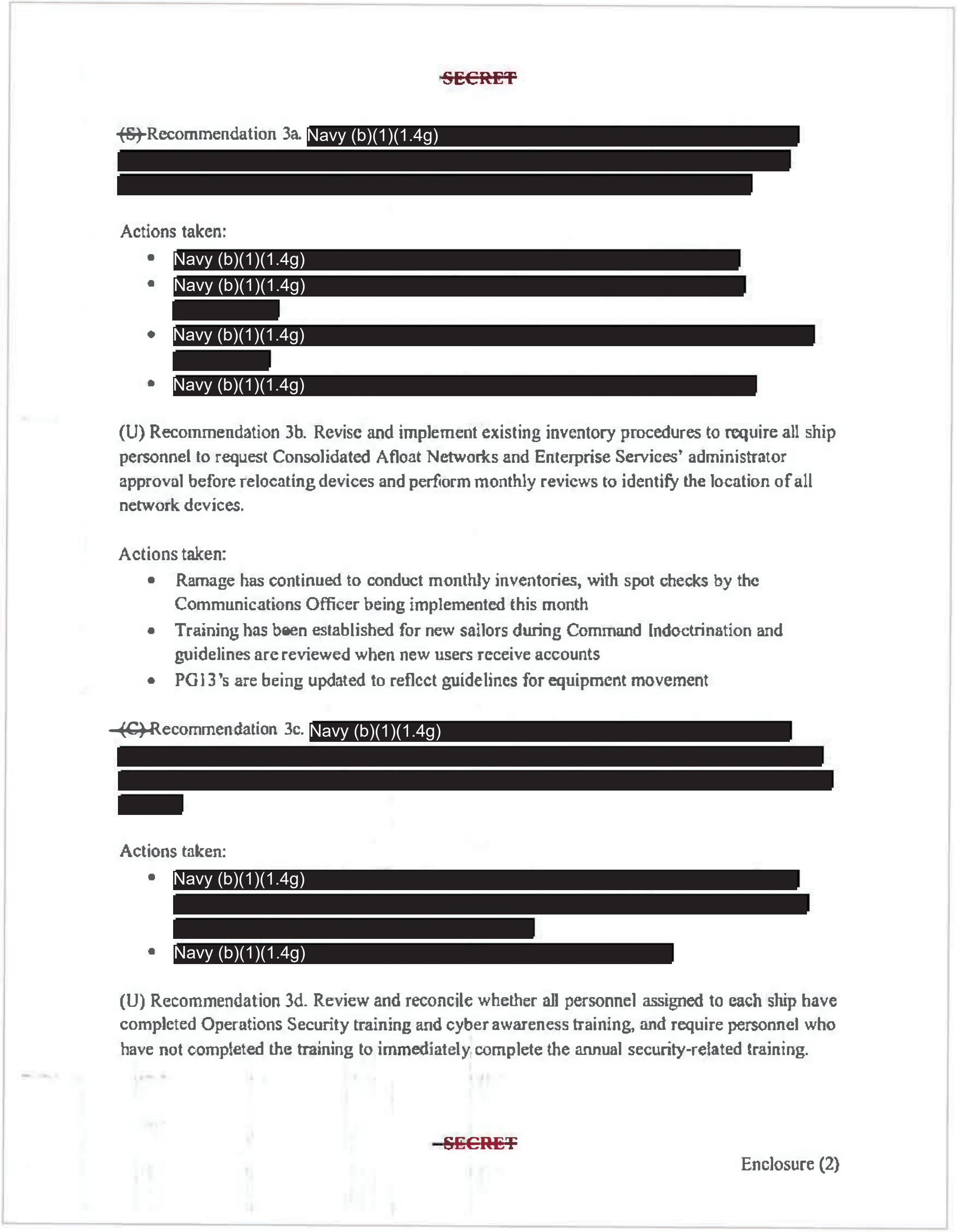
1. I have reviewed paragraphs three, four, and six of enclosure (1). I am responding as Immediate Superior in Command (ISIC) of USS RAMAGE (DDG 61). I agree with the recommendations that were made in paragraphs three, four, and six.

2. Enclosure (2) written in January 2019 details action taken by RAMAGE to address and mitigate recommendations of enclosure (1) in paragraphs three, four, and six. RAMAGE has fulfilled all required actions to Department of Defense Inspector General recommendations in paragraphs three, four, and six.

3. If there are any questions my point of contact is [redacted], he can be reached at [redacted] or by email at [redacted].

Navy (b)(6)

## (U) Destroyer Squadron Two Eight (cont'd)



~~SECRET~~

~~(S)~~ Recommendation 3a. Navy (b)(1)(1.4g)

Actions taken:

- Navy (b)(1)(1.4g)
- Navy (b)(1)(1.4g)
- Navy (b)(1)(1.4g)
- Navy (b)(1)(1.4g)

(U) Recommendation 3b. Revise and implement existing inventory procedures to require all ship personnel to request Consolidated Afloat Networks and Enterprise Services' administrator approval before relocating devices and perform monthly reviews to identify the location of all network devices.

Actions taken:

- Ramage has continued to conduct monthly inventories, with spot checks by the Communications Officer being implemented this month
- Training has been established for new sailors during Command Indoctrination and guidelines are reviewed when new users receive accounts
- PG13's are being updated to reflect guidelines for equipment movement

~~(C)~~ Recommendation 3c. Navy (b)(1)(1.4g)

Actions taken:

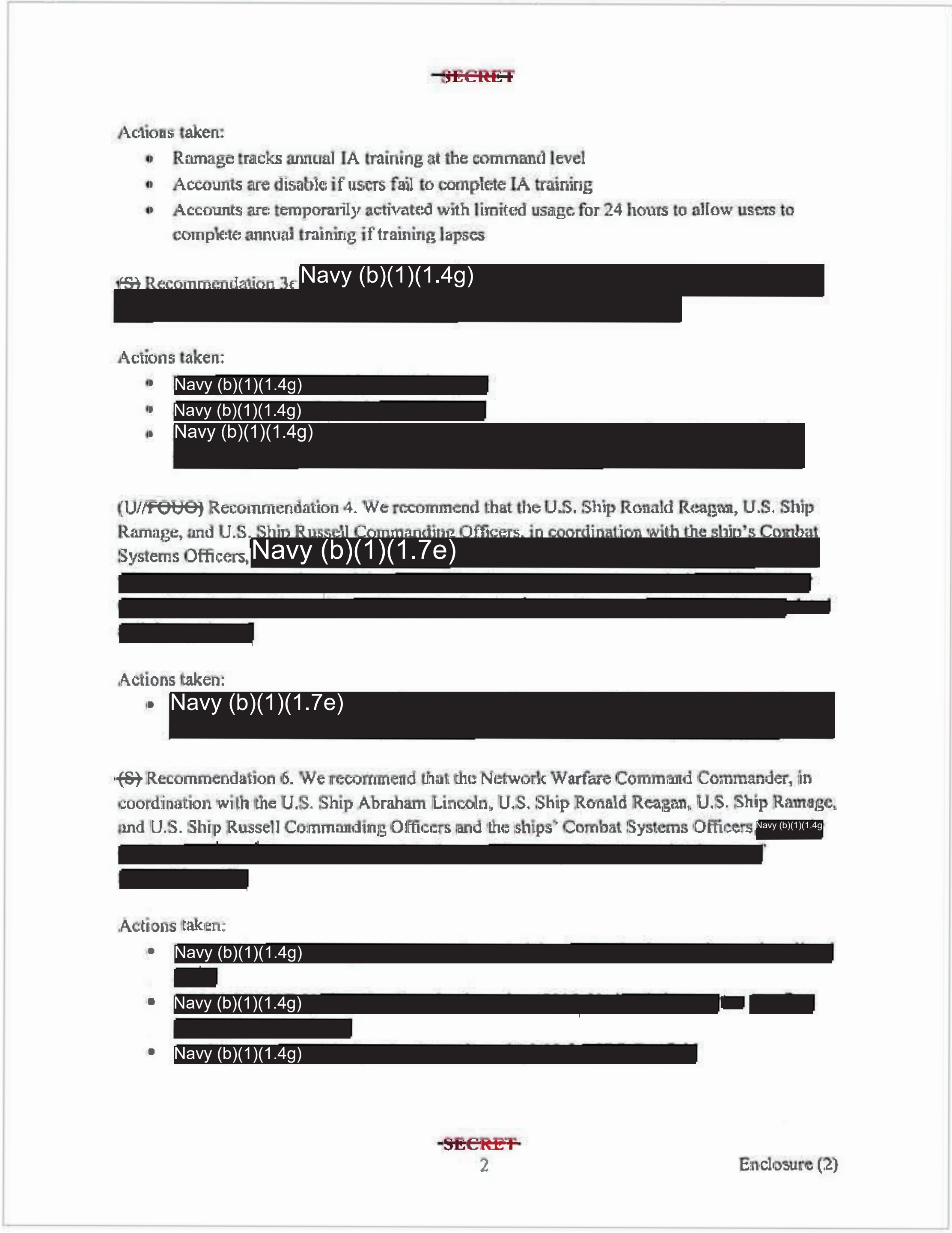
- Navy (b)(1)(1.4g)
- Navy (b)(1)(1.4g)

(U) Recommendation 3d. Review and reconcile whether all personnel assigned to each ship have completed Operations Security training and cyber awareness training, and require personnel who have not completed the training to immediately complete the annual security-related training.

~~SECRET~~

Enclosure (2)

# (U) Destroyer Squadron Two Eight (cont'd)



~~SECRET~~

Actions taken:

- Ramage tracks annual IA training at the command level
- Accounts are disable if users fail to complete IA training
- Accounts are temporarily activated with limited usage for 24 hours to allow users to complete annual training if training lapses

~~(S)~~ Recommendation 3c Navy (b)(1)(1.4g)

Actions taken:

- Navy (b)(1)(1.4g)
- Navy (b)(1)(1.4g)
- Navy (b)(1)(1.4g)

(U//~~FOUO~~) Recommendation 4. We recommend that the U.S. Ship Ronald Reagan, U.S. Ship Ramage, and U.S. Ship Russell Commanding Officers, in coordination with the ship's Combat Systems Officers, Navy (b)(1)(1.7e)

Actions taken:

- Navy (b)(1)(1.7e)

~~(S)~~ Recommendation 6. We recommend that the Network Warfare Command Commander, in coordination with the U.S. Ship Abraham Lincoln, U.S. Ship Ronald Reagan, U.S. Ship Ramage, and U.S. Ship Russell Commanding Officers and the ships' Combat Systems Officers Navy (b)(1)(1.4g

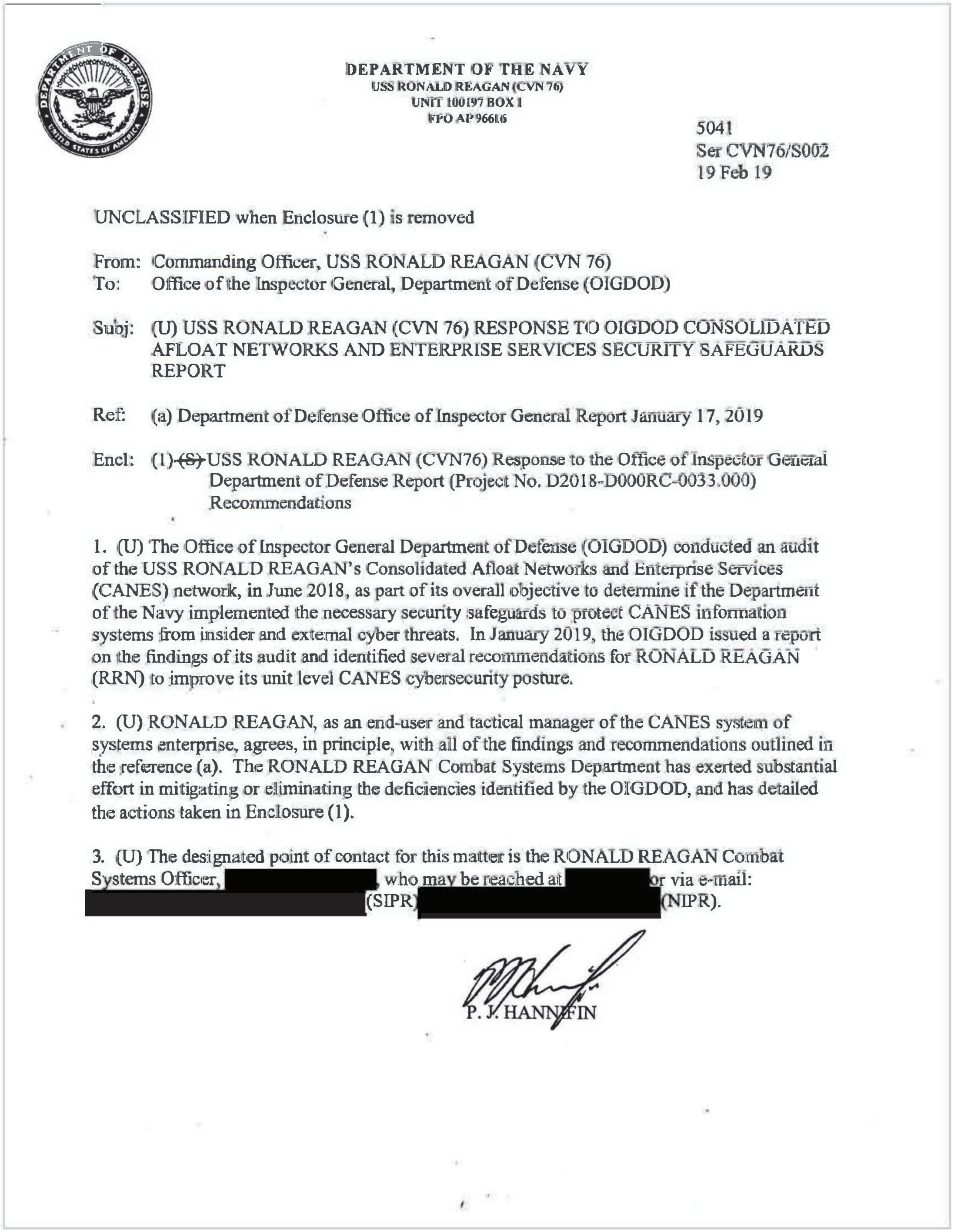
Actions taken:

- Navy (b)(1)(1.4g)
- Navy (b)(1)(1.4g)
- Navy (b)(1)(1.4g)

~~SECRET~~

2 Enclosure (2)

## (U) USS *Ronald Reagan*



DEPARTMENT OF THE NAVY
USS RONALD REAGAN (CVN 76)
UNIT 100197 BOX 1
FPO AP 96616

5041
Ser CVN76/S002
19 Feb 19

UNCLASSIFIED when Enclosure (1) is removed

From: Commanding Officer, USS RONALD REAGAN (CVN 76)
To: Office of the Inspector General, Department of Defense (OIGDOD)

Subj: (U) USS RONALD REAGAN (CVN 76) RESPONSE TO OIGDOD CONSOLIDATED AFLOAT NETWORKS AND ENTERPRISE SERVICES SECURITY SAFEGUARDS REPORT

Ref: (a) Department of Defense Office of Inspector General Report January 17, 2019

Encl: (1) ~~(S)~~ USS RONALD REAGAN (CVN76) Response to the Office of Inspector General Department of Defense Report (Project No. D2018-D000RC-0033.000) Recommendations

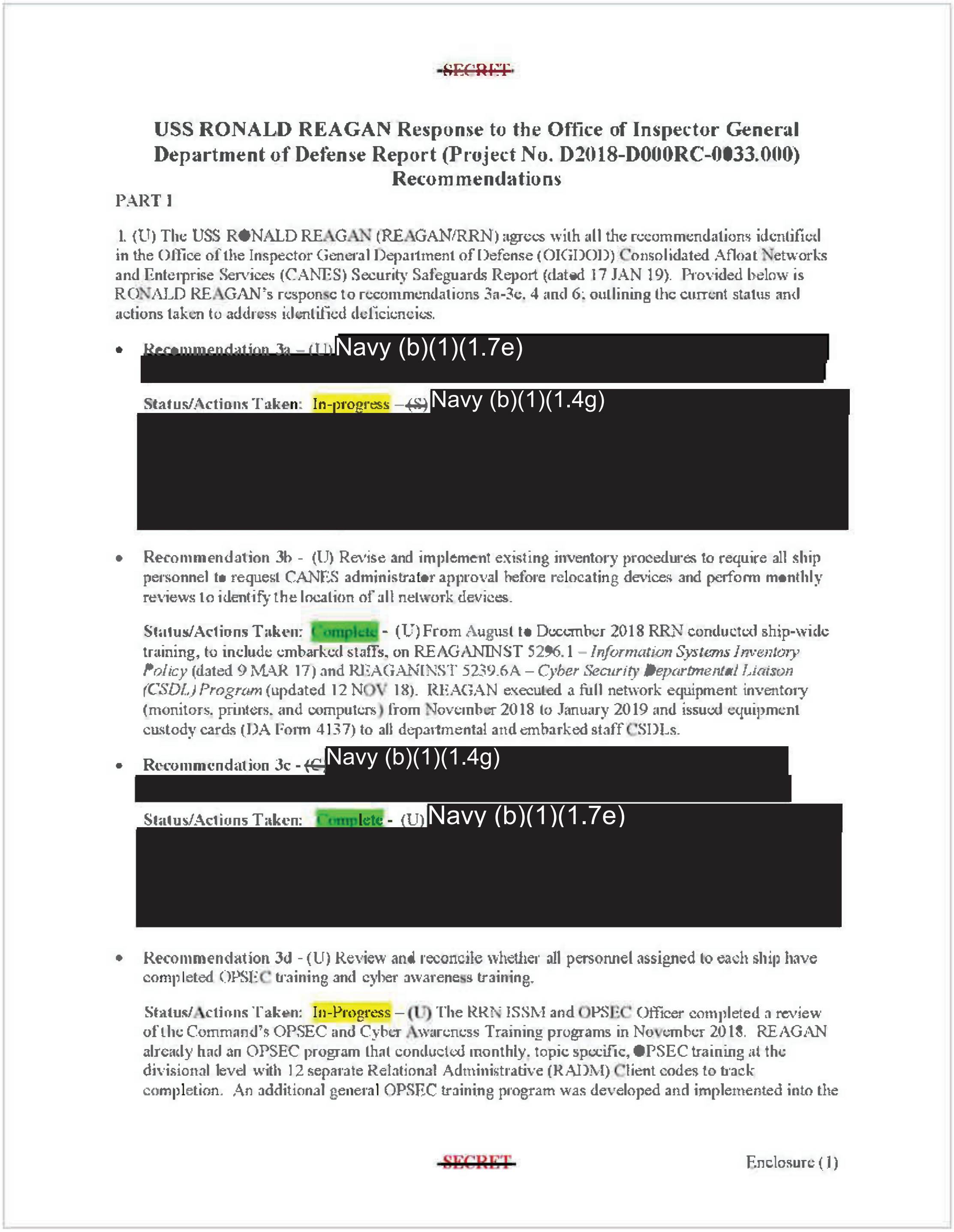
1. (U) The Office of Inspector General Department of Defense (OIGDOD) conducted an audit of the USS RONALD REAGAN's Consolidated Afloat Networks and Enterprise Services (CANES) network, in June 2018, as part of its overall objective to determine if the Department of the Navy implemented the necessary security safeguards to protect CANES information systems from insider and external cyber threats. In January 2019, the OIGDOD issued a report on the findings of its audit and identified several recommendations for RONALD REAGAN (RRN) to improve its unit level CANES cybersecurity posture.

2. (U) RONALD REAGAN, as an end-user and tactical manager of the CANES system of systems enterprise, agrees, in principle, with all of the findings and recommendations outlined in the reference (a). The RONALD REAGAN Combat Systems Department has exerted substantial effort in mitigating or eliminating the deficiencies identified by the OIGDOD, and has detailed the actions taken in Enclosure (1).

3. (U) The designated point of contact for this matter is the RONALD REAGAN Combat Systems Officer, [redacted], who may be reached at [redacted] or via e-mail: [redacted] (SIPR) [redacted] (NIPR).

P. J. HANNIFIN

# (U) USS *Ronald Reagan* (cont'd)



~~SECRET~~

**USS RONALD REAGAN Response to the Office of Inspector General Department of Defense Report (Project No. D2018-D000RC-0033.000) Recommendations**

PART 1

1. (U) The USS RONALD REAGAN (REAGAN/RRN) agrees with all the recommendations identified in the Office of the Inspector General Department of Defense (OIGDOD) Consolidated Afloat Networks and Enterprise Services (CANES) Security Safeguards Report (dated 17 JAN 19). Provided below is RONALD REAGAN's response to recommendations 3a-3c, 4 and 6; outlining the current status and actions taken to address identified deficiencies.

- Recommendation 3a – (U) Navy (b)(1)(1.7e)

  Status/Actions Taken: In-progress – ~~(S)~~ Navy (b)(1)(1.4g)

- Recommendation 3b - (U) Revise and implement existing inventory procedures to require all ship personnel to request CANES administrator approval before relocating devices and perform monthly reviews to identify the location of all network devices.

  Status/Actions Taken: Complete - (U) From August to December 2018 RRN conducted ship-wide training, to include embarked staffs, on REAGANINST 5296.1 – *Information Systems Inventory Policy* (dated 9 MAR 17) and REAGANINST 5239.6A – *Cyber Security Departmental Liaison (CSDL) Program* (updated 12 NOV 18). REAGAN executed a full network equipment inventory (monitors, printers, and computers) from November 2018 to January 2019 and issued equipment custody cards (DA Form 4137) to all departmental and embarked staff CSDLs.

- Recommendation 3c - (C Navy (b)(1)(1.4g)

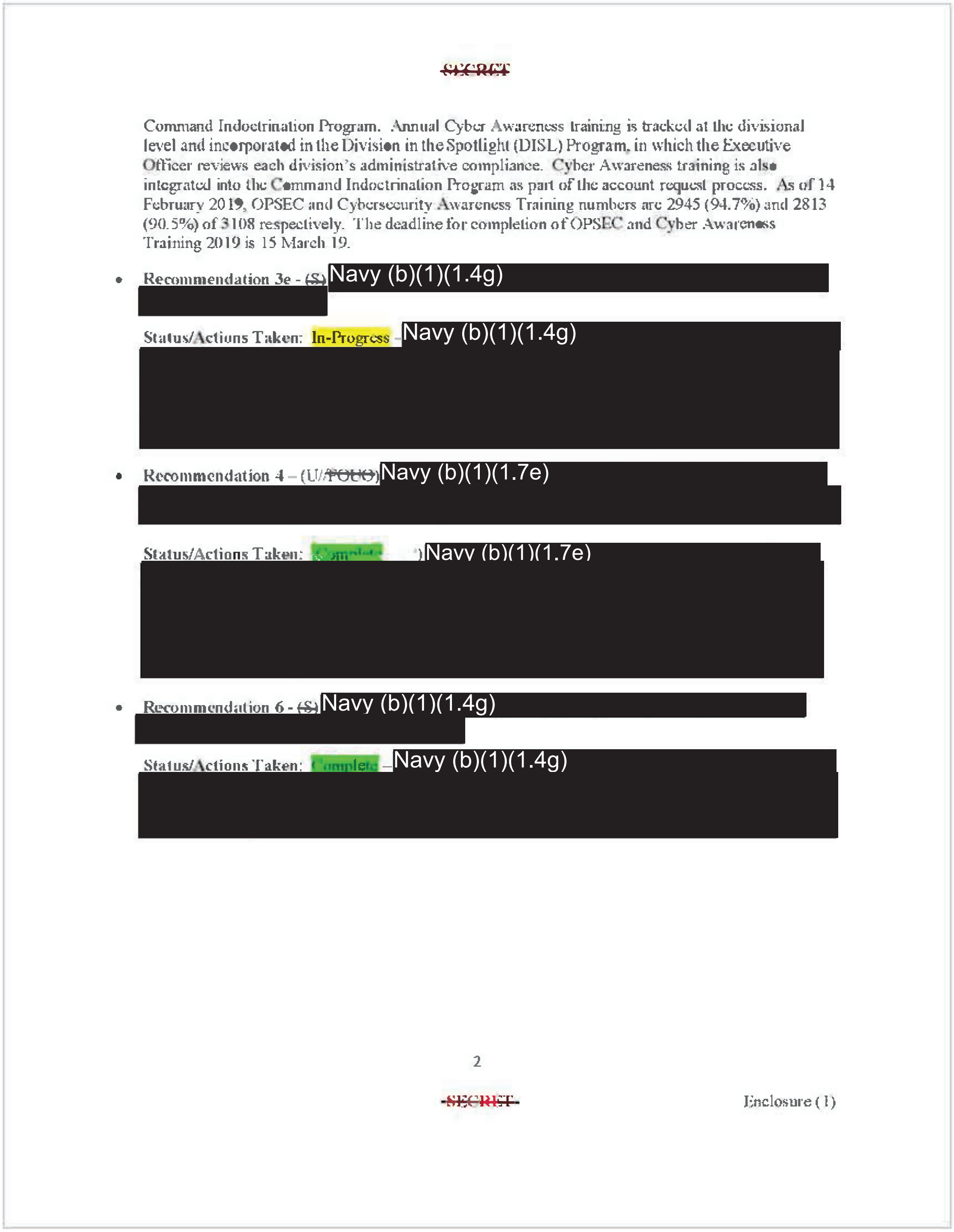
  Status/Actions Taken: Complete - (U) Navy (b)(1)(1.7e)

- Recommendation 3d - (U) Review and reconcile whether all personnel assigned to each ship have completed OPSEC training and cyber awareness training.

  Status/Actions Taken: In-Progress – (U) The RRN ISSM and OPSEC Officer completed a review of the Command's OPSEC and Cyber Awareness Training programs in November 2018. REAGAN already had an OPSEC program that conducted monthly, topic specific, OPSEC training at the divisional level with 12 separate Relational Administrative (RADM) Client codes to track completion. An additional general OPSEC training program was developed and implemented into the

~~SECRET~~ Enclosure (1)

## (U) USS *Ronald Reagan* (cont'd)



Command Indoctrination Program. Annual Cyber Awareness training is tracked at the divisional level and incorporated in the Division in the Spotlight (DISL) Program, in which the Executive Officer reviews each division's administrative compliance. Cyber Awareness training is also integrated into the Command Indoctrination Program as part of the account request process. As of 14 February 2019, OPSEC and Cybersecurity Awareness Training numbers are 2945 (94.7%) and 2813 (90.5%) of 3108 respectively. The deadline for completion of OPSEC and Cyber Awareness Training 2019 is 15 March 19.

- **Recommendation 3e** - ~~(S)~~ Navy (b)(1)(1.4g)

  **Status/Actions Taken:** **In-Progress** – Navy (b)(1)(1.4g)

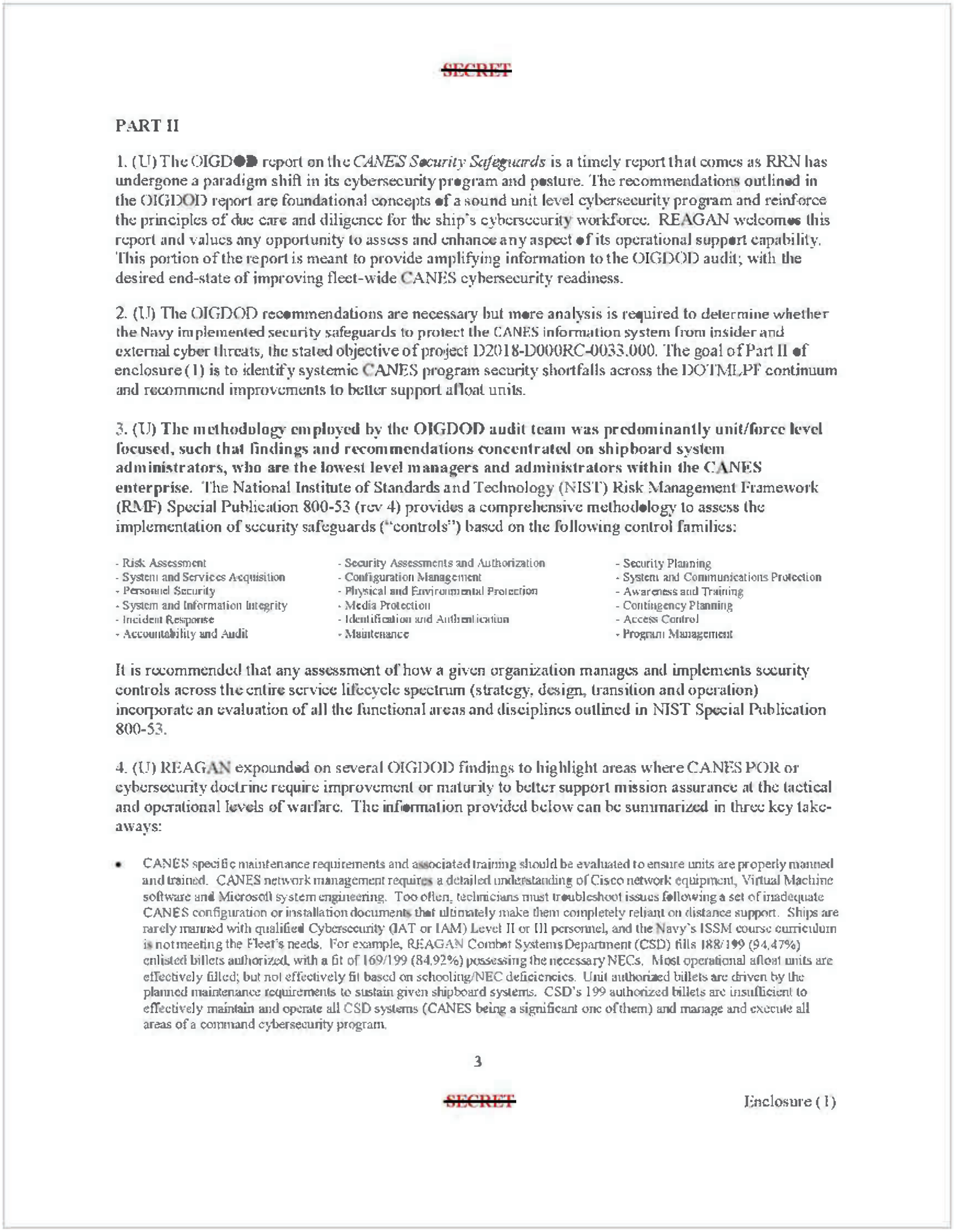
- **Recommendation 4** – (U/~~FOUO~~) Navy (b)(1)(1.7e)

  **Status/Actions Taken:** **Complete** – )Navy (b)(1)(1.7e)

- **Recommendation 6** - ~~(S)~~ Navy (b)(1)(1.4g)

  **Status/Actions Taken:** **Complete** – Navy (b)(1)(1.4g)

# (U) USS *Ronald Reagan* (cont'd)



~~SECRET~~

PART II

1. (U) The OIGDOD report on the *CANES Security Safeguards* is a timely report that comes as RRN has undergone a paradigm shift in its cybersecurity program and posture. The recommendations outlined in the OIGDOD report are foundational concepts of a sound unit level cybersecurity program and reinforce the principles of due care and diligence for the ship's cybersecurity workforce. REAGAN welcomes this report and values any opportunity to assess and enhance any aspect of its operational support capability. This portion of the report is meant to provide amplifying information to the OIGDOD audit; with the desired end-state of improving fleet-wide CANES cybersecurity readiness.

2. (U) The OIGDOD recommendations are necessary but more analysis is required to determine whether the Navy implemented security safeguards to protect the CANES information system from insider and external cyber threats, the stated objective of project D2018-D000RC-0033.000. The goal of Part II of enclosure (1) is to identify systemic CANES program security shortfalls across the DOTMLPF continuum and recommend improvements to better support afloat units.

3. (U) The methodology employed by the OIGDOD audit team was predominantly unit/force level focused, such that findings and recommendations concentrated on shipboard system administrators, who are the lowest level managers and administrators within the CANES enterprise. The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) Special Publication 800-53 (rev 4) provides a comprehensive methodology to assess the implementation of security safeguards ("controls") based on the following control families:

- Risk Assessment
- System and Services Acquisition
- Personnel Security
- System and Information Integrity
- Incident Response
- Accountability and Audit
- Security Assessments and Authorization
- Configuration Management
- Physical and Environmental Protection
- Media Protection
- Identification and Authentication
- Maintenance
- Security Planning
- System and Communications Protection
- Awareness and Training
- Contingency Planning
- Access Control
- Program Management

It is recommended that any assessment of how a given organization manages and implements security controls across the entire service lifecycle spectrum (strategy, design, transition and operation) incorporate an evaluation of all the functional areas and disciplines outlined in NIST Special Publication 800-53.

4. (U) REAGAN expounded on several OIGDOD findings to highlight areas where CANES POR or cybersecurity doctrine require improvement or maturity to better support mission assurance at the tactical and operational levels of warfare. The information provided below can be summarized in three key take-aways:

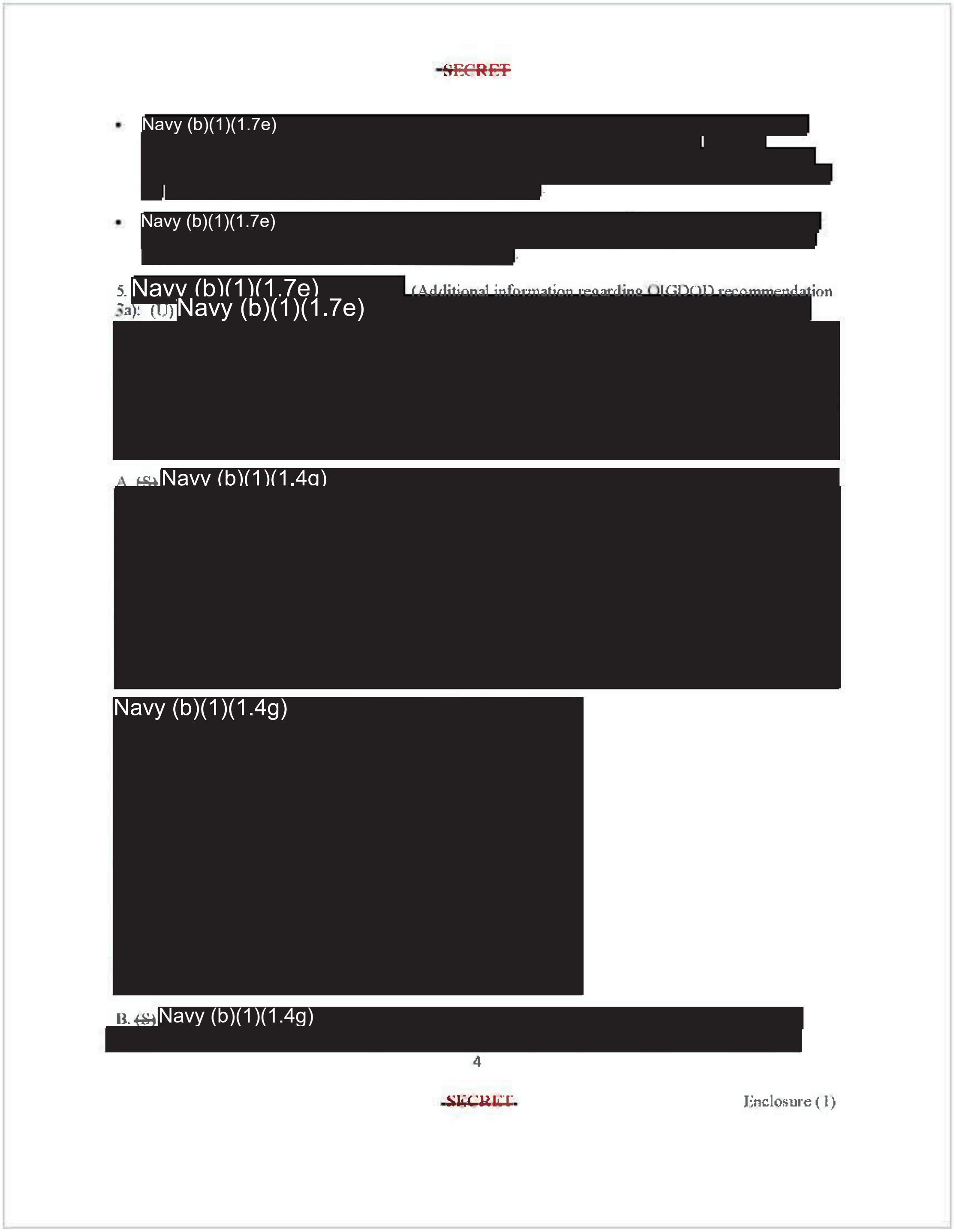
- CANES specific maintenance requirements and associated training should be evaluated to ensure units are properly manned and trained. CANES network management requires a detailed understanding of Cisco network equipment, Virtual Machine software and Microsoft system engineering. Too often, technicians must troubleshoot issues following a set of inadequate CANES configuration or installation documents that ultimately make them completely reliant on distance support. Ships are rarely manned with qualified Cybersecurity (IAT or IAM) Level II or III personnel, and the Navy's ISSM course curriculum is not meeting the Fleet's needs. For example, REAGAN Combat Systems Department (CSD) fills 188/199 (94.47%) enlisted billets authorized, with a fit of 169/199 (84.92%) possessing the necessary NECs. Most operational afloat units are effectively filled; but not effectively fit based on schooling/NEC deficiencies. Unit authorized billets are driven by the planned maintenance requirements to sustain given shipboard systems. CSD's 199 authorized billets are insufficient to effectively maintain and operate all CSD systems (CANES being a significant one of them) and manage and execute all areas of a command cybersecurity program.

3

~~SECRET~~

Enclosure (1)

# (U) USS *Ronald Reagan* (cont'd)



~~SECRET~~

- Navy (b)(1)(1.7e) [redacted]
- Navy (b)(1)(1.7e) [redacted]

5. Navy (b)(1)(1.7e) [redacted] (Additional information regarding OIGDOD recommendation 3a): (U) Navy (b)(1)(1.7e) [redacted]

A. ~~(S)~~ Navy (b)(1)(1.4g) [redacted]

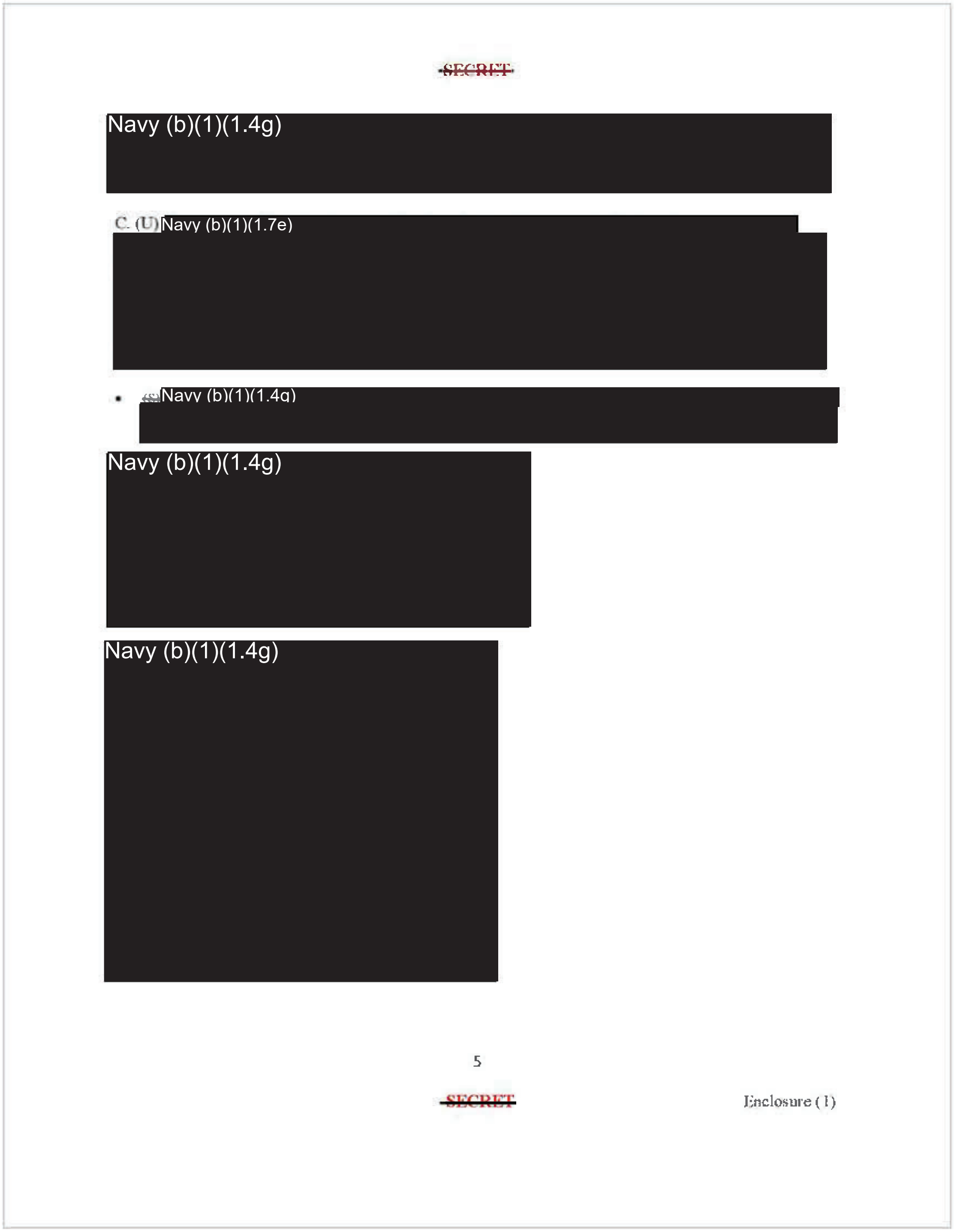
Navy (b)(1)(1.4g) [redacted]

B. ~~(S)~~ Navy (b)(1)(1.4g) [redacted]

4

~~SECRET~~ Enclosure (1)

## (U) USS *Ronald Reagan* (cont'd)



~~SECRET~~

Navy (b)(1)(1.4g) [redacted]

C. (U) Navy (b)(1)(1.7e) [redacted]

- (S) Navy (b)(1)(1.4g) [redacted]

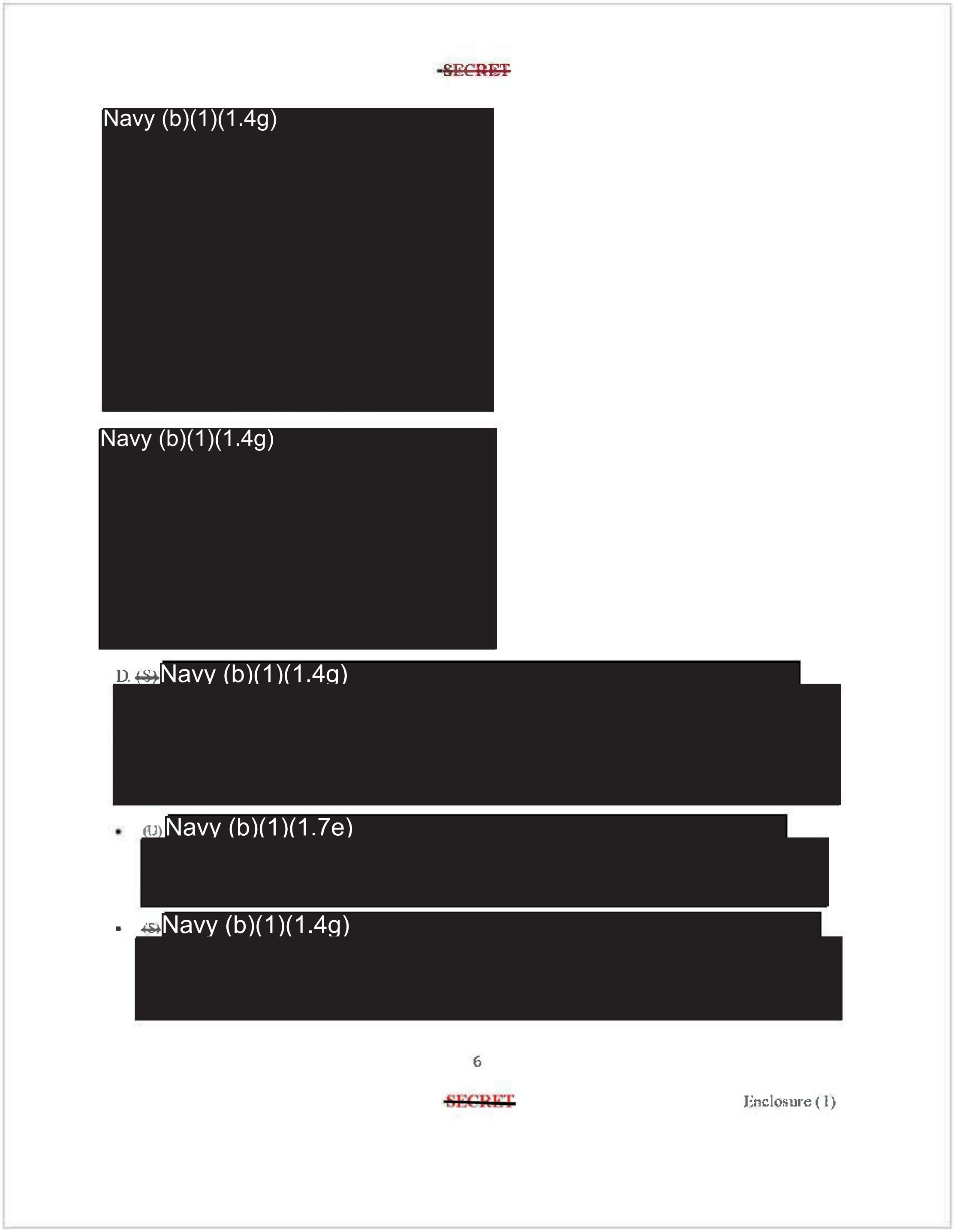
Navy (b)(1)(1.4g) [redacted]

Navy (b)(1)(1.4g) [redacted]

5

~~SECRET~~ Enclosure (1)

## (U) USS *Ronald Reagan* (cont'd)



~~SECRET~~

Navy (b)(1)(1.4g) [redacted]

Navy (b)(1)(1.4g) [redacted]

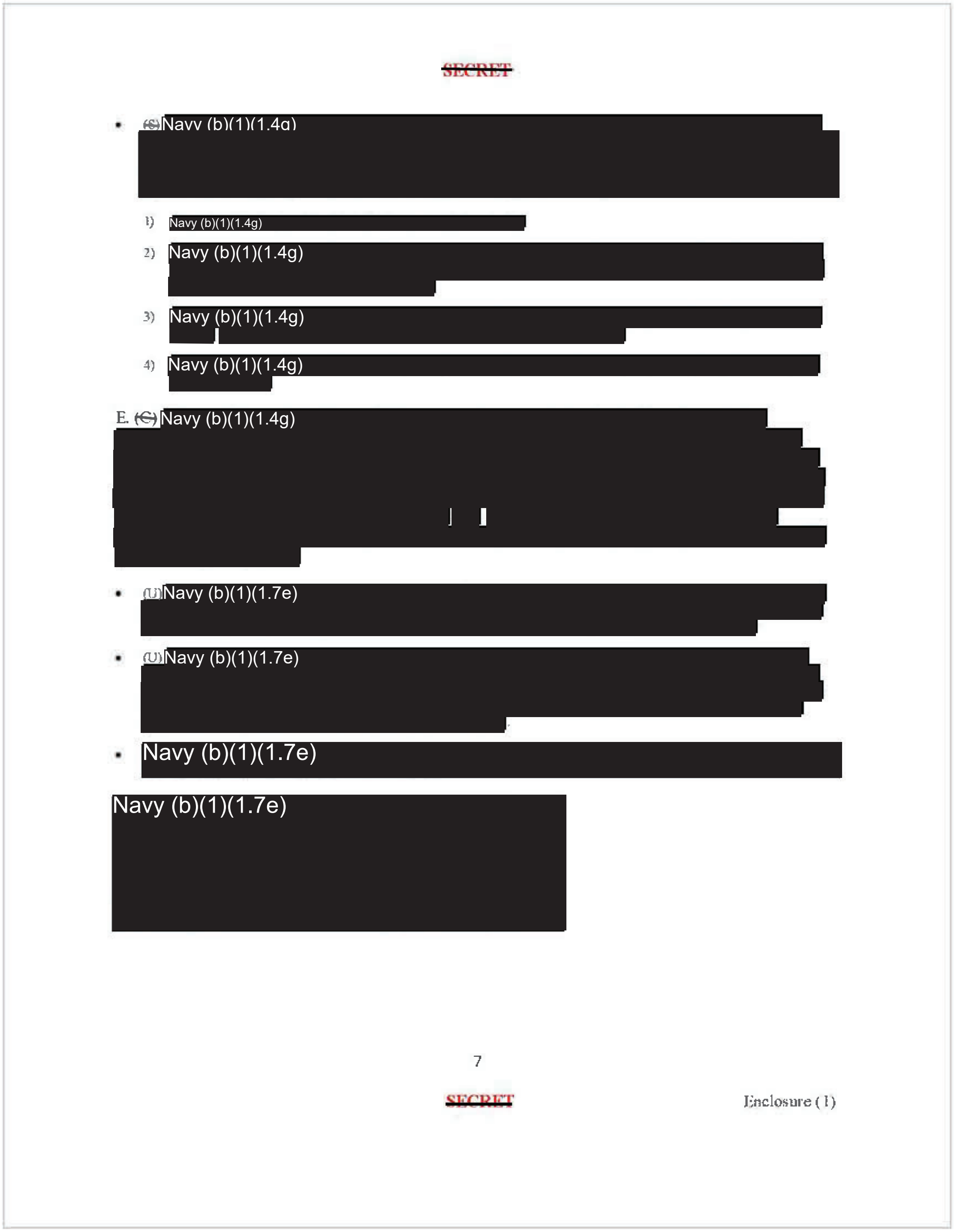
D. ~~(S)~~ Navy (b)(1)(1.4g) [redacted]

- (U) Navy (b)(1)(1.7e) [redacted]
- ~~(S)~~ Navy (b)(1)(1.4g) [redacted]

6

~~SECRET~~ Enclosure (1)

# (U) USS *Ronald Reagan* (cont'd)



~~SECRET~~

- (S) Navy (b)(1)(1.4g)

    1) Navy (b)(1)(1.4g)

    2) Navy (b)(1)(1.4g)

    3) Navy (b)(1)(1.4g)

    4) Navy (b)(1)(1.4g)

E. ~~(C)~~ Navy (b)(1)(1.4g)

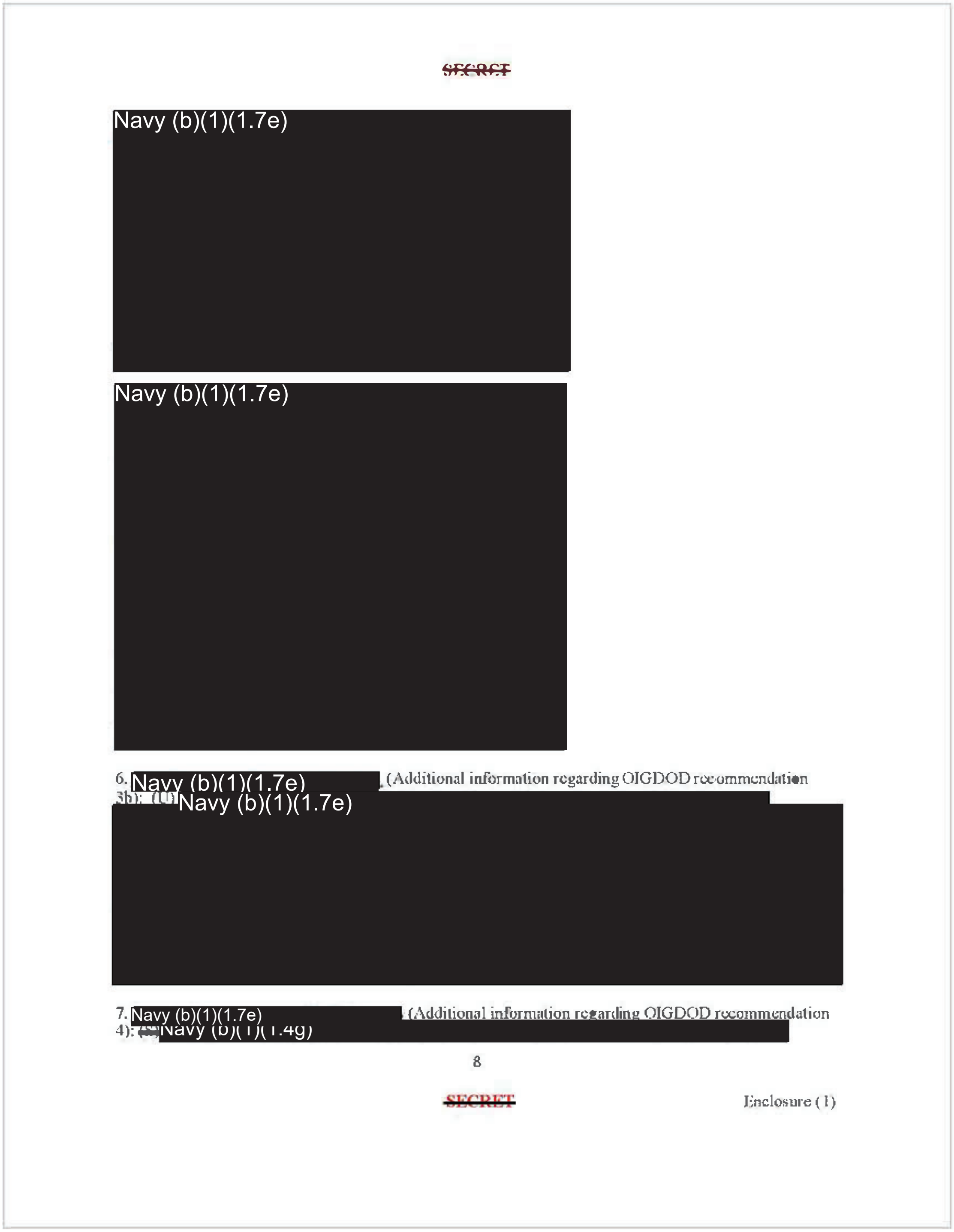
- (U) Navy (b)(1)(1.7e)
- (U) Navy (b)(1)(1.7e)
- Navy (b)(1)(1.7e)

Navy (b)(1)(1.7e)

7

~~SECRET~~ Enclosure (1)

# (U) USS Ronald Reagan (cont'd)



~~SECRET~~

Navy (b)(1)(1.7e) [redacted]

Navy (b)(1)(1.7e) [redacted]

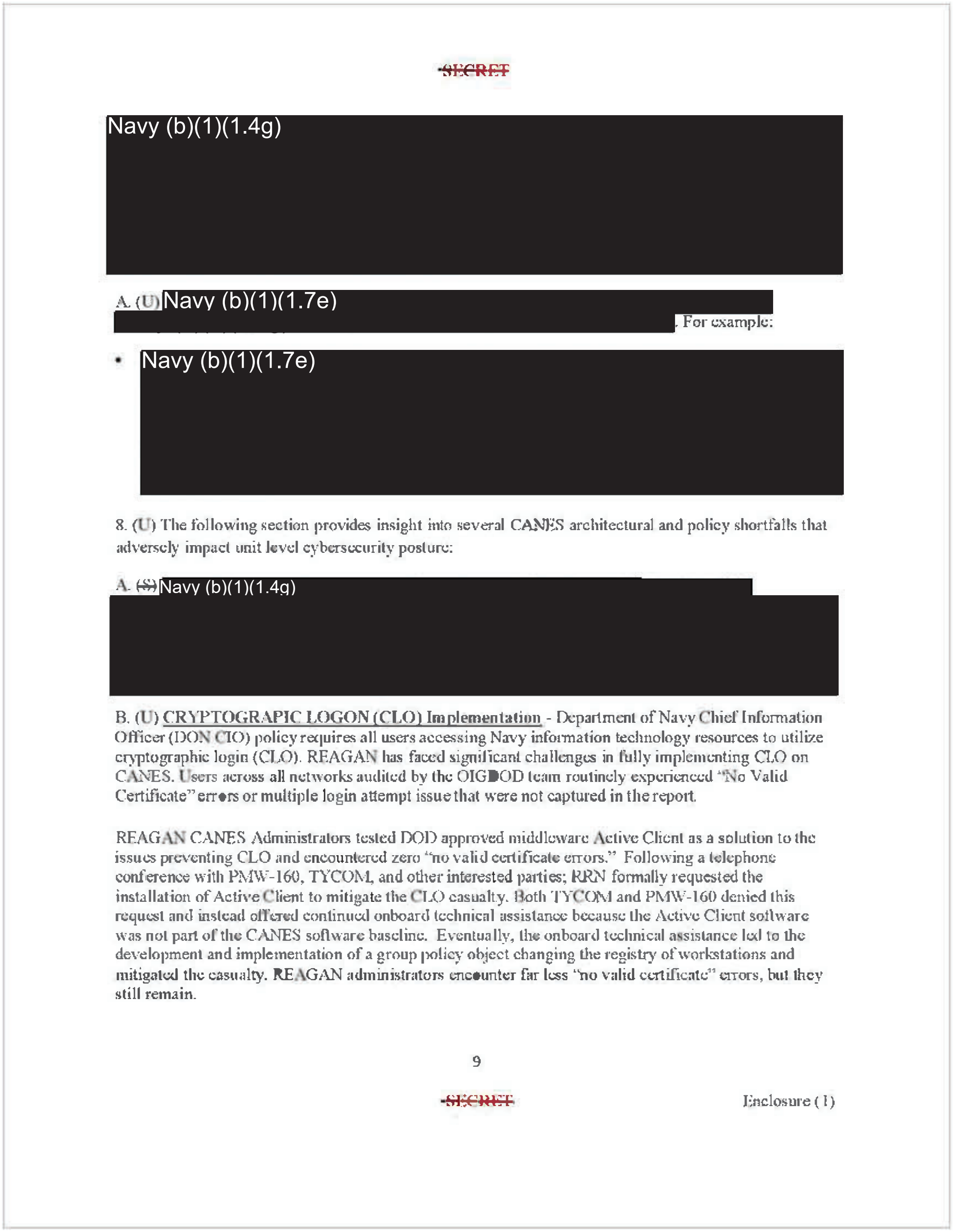
6. Navy (b)(1)(1.7e) [redacted] (Additional information regarding OIGDOD recommendation 3b): (U) Navy (b)(1)(1.7e) [redacted]

7. Navy (b)(1)(1.7e) [redacted] (Additional information regarding OIGDOD recommendation 4): Navy (b)(1)(1.4g) [redacted]

8

~~SECRET~~ Enclosure (1)

## (U) USS *Ronald Reagan* (cont'd)



Navy (b)(1)(1.4g)

A. (U) Navy (b)(1)(1.7e) . For example:

- Navy (b)(1)(1.7e)

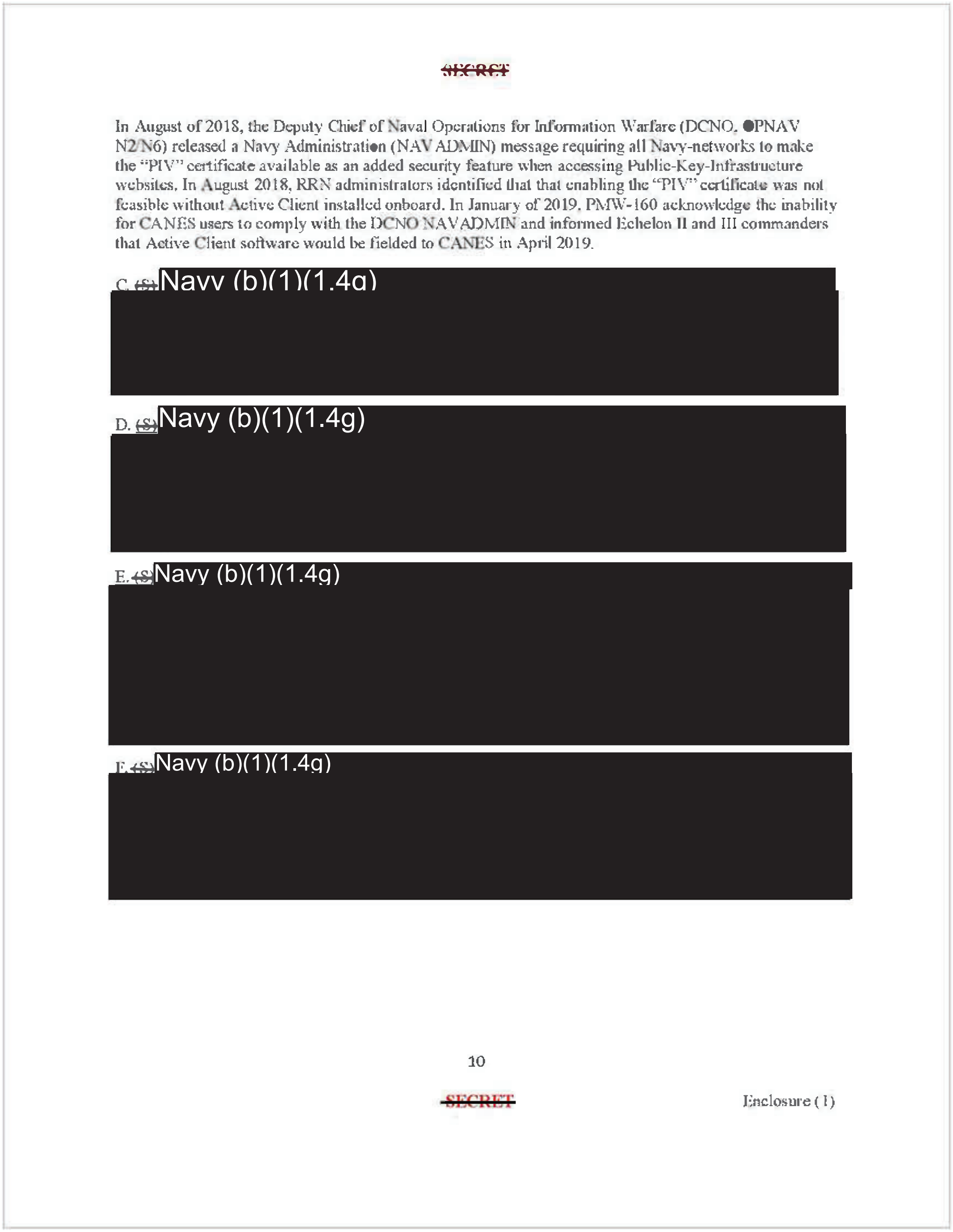
8. (U) The following section provides insight into several CANES architectural and policy shortfalls that adversely impact unit level cybersecurity posture:

A. ~~(S)~~ Navy (b)(1)(1.4g)

B. (U) CRYPTOGRAPIC LOGON (CLO) Implementation - Department of Navy Chief Information Officer (DON CIO) policy requires all users accessing Navy information technology resources to utilize cryptographic login (CLO). REAGAN has faced significant challenges in fully implementing CLO on CANES. Users across all networks audited by the OIGDOD team routinely experienced "No Valid Certificate" errors or multiple login attempt issue that were not captured in the report.

REAGAN CANES Administrators tested DOD approved middleware Active Client as a solution to the issues preventing CLO and encountered zero "no valid certificate errors." Following a telephone conference with PMW-160, TYCOM, and other interested parties; RRN formally requested the installation of Active Client to mitigate the CLO casualty. Both TYCOM and PMW-160 denied this request and instead offered continued onboard technical assistance because the Active Client software was not part of the CANES software baseline. Eventually, the onboard technical assistance led to the development and implementation of a group policy object changing the registry of workstations and mitigated the casualty. REAGAN administrators encounter far less "no valid certificate" errors, but they still remain.

## (U) USS *Ronald Reagan* (cont'd)



~~SECRET~~

In August of 2018, the Deputy Chief of Naval Operations for Information Warfare (DCNO, ●PNAV N2/N6) released a Navy Administrati●n (NAVADMIN) message requiring all Navy-networks to make the "PIV" certificate available as an added security feature when accessing Public-Key-Infrastructure websites. In August 2018, RRN administrators identified that that enabling the "PIV" certificate was not feasible without Active Client installed onboard. In January of 2019, PMW-160 acknowledge the inability for CANES users to comply with the DCNO NAVADMIN and informed Echelon II and III commanders that Active Client software would be fielded to CANES in April 2019.

C. ~~(S)~~ Navy (b)(1)(1.4g) [redacted]

D. ~~(S)~~ Navy (b)(1)(1.4g) [redacted]

E. ~~(S)~~ Navy (b)(1)(1.4g) [redacted]

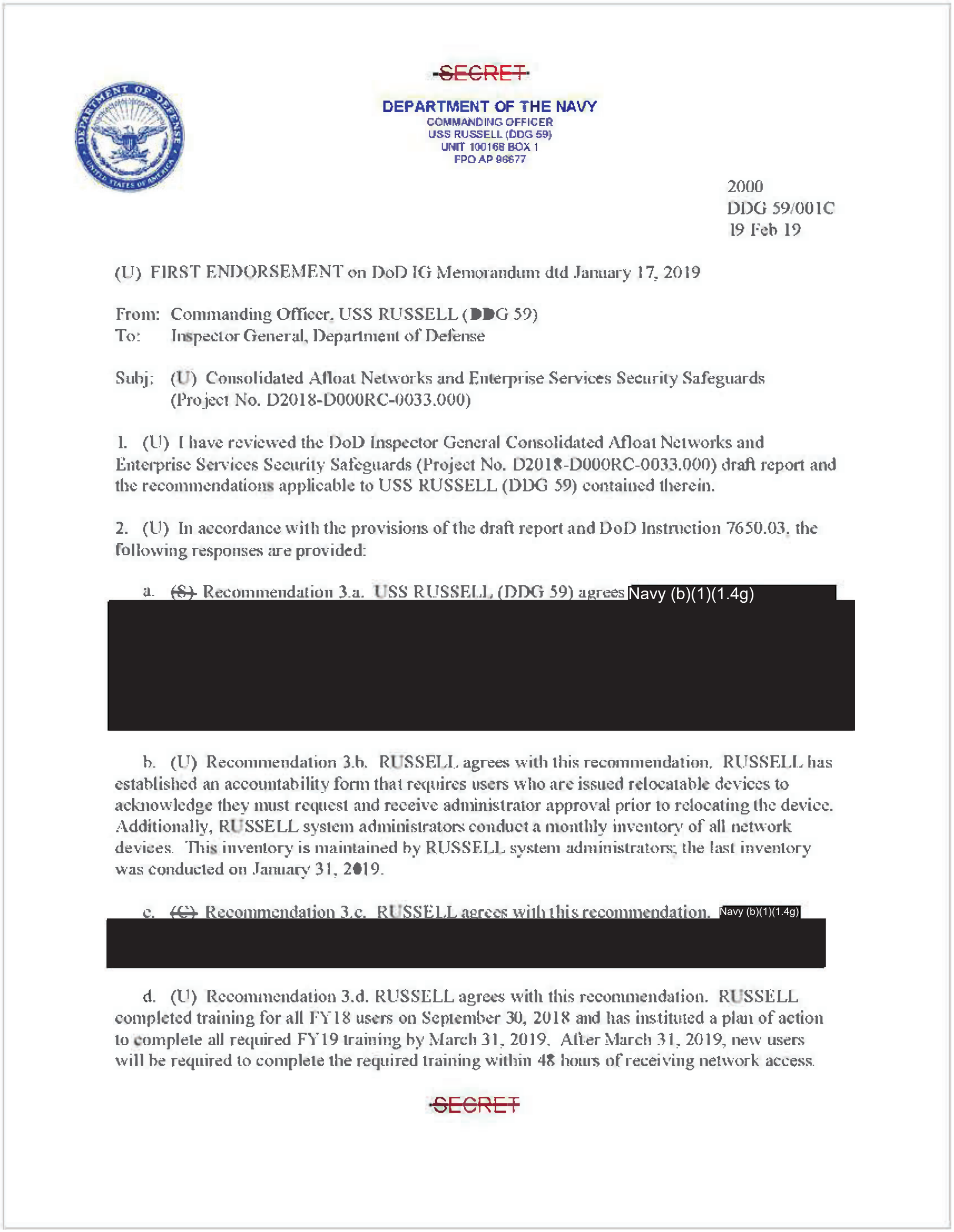
F. ~~(S)~~ Navy (b)(1)(1.4g) [redacted]

10

~~SECRET~~

Enclosure (1)

# (U) USS *Russell*



~~SECRET~~

DEPARTMENT OF THE NAVY
COMMANDING OFFICER
USS RUSSELL (DDG 59)
UNIT 100168 BOX 1
FPO AP 96677

2000
DDG 59/001C
19 Feb 19

(U) FIRST ENDORSEMENT on DoD IG Memorandum dtd January 17, 2019

From: Commanding Officer, USS RUSSELL (DDG 59)
To: Inspector General, Department of Defense

Subj: (U) Consolidated Afloat Networks and Enterprise Services Security Safeguards (Project No. D2018-D000RC-0033.000)

1. (U) I have reviewed the DoD Inspector General Consolidated Afloat Networks and Enterprise Services Security Safeguards (Project No. D2018-D000RC-0033.000) draft report and the recommendations applicable to USS RUSSELL (DDG 59) contained therein.

2. (U) In accordance with the provisions of the draft report and DoD Instruction 7650.03, the following responses are provided:

a. (~~S~~) Recommendation 3.a. USS RUSSELL (DDG 59) agrees Navy (b)(1)(1.4g) [redacted]

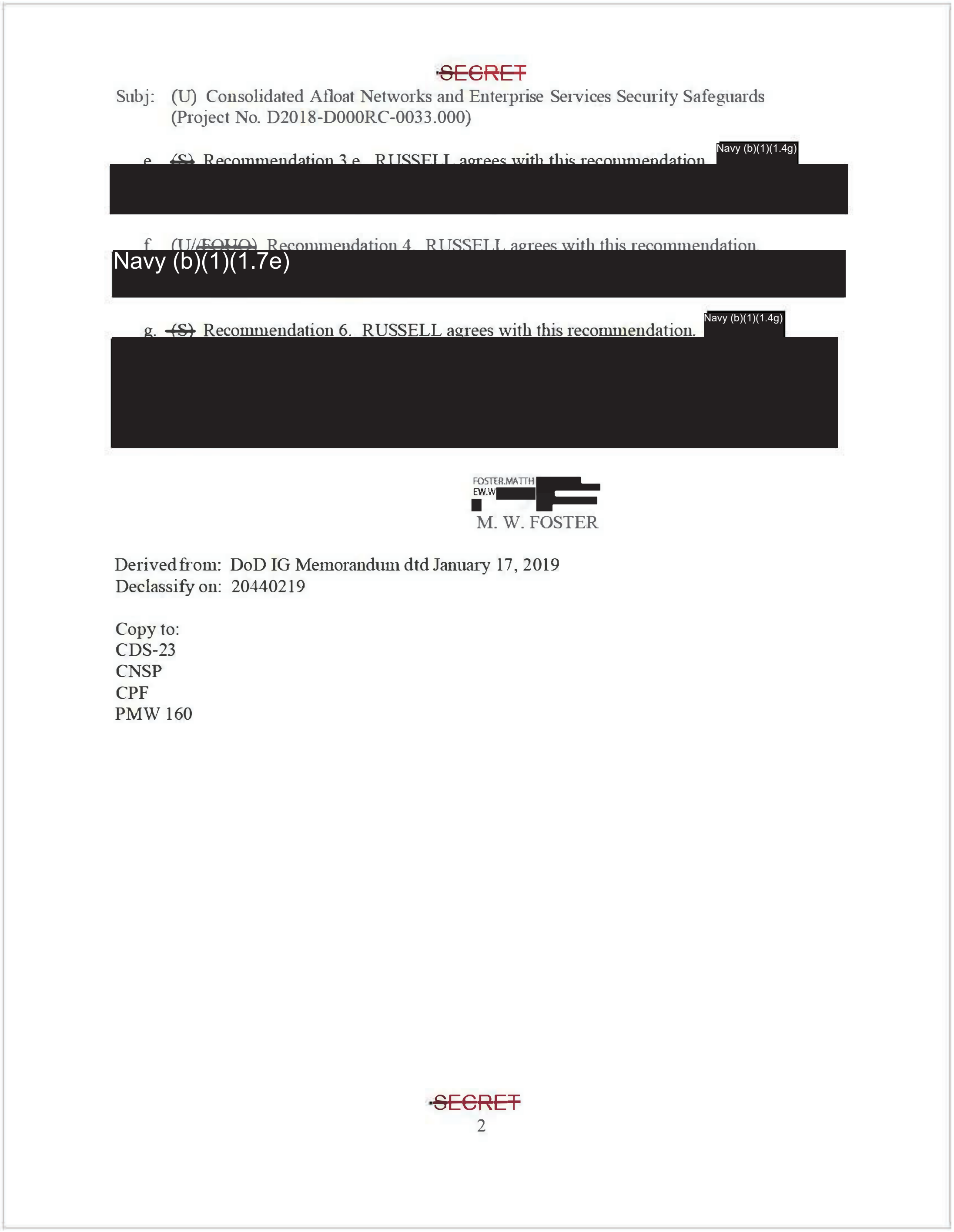
b. (U) Recommendation 3.b. RUSSELL agrees with this recommendation. RUSSELL has established an accountability form that requires users who are issued relocatable devices to acknowledge they must request and receive administrator approval prior to relocating the device. Additionally, RUSSELL system administrators conduct a monthly inventory of all network devices. This inventory is maintained by RUSSELL system administrators; the last inventory was conducted on January 31, 2019.

c. (~~C~~) Recommendation 3.c. RUSSELL agrees with this recommendation. Navy (b)(1)(1.4g) [redacted]

d. (U) Recommendation 3.d. RUSSELL agrees with this recommendation. RUSSELL completed training for all FY18 users on September 30, 2018 and has instituted a plan of action to complete all required FY19 training by March 31, 2019. After March 31, 2019, new users will be required to complete the required training within 48 hours of receiving network access.

~~SECRET~~

## (U) USS *Russell* (cont’d)



~~SECRET~~

Subj: (U) Consolidated Afloat Networks and Enterprise Services Security Safeguards (Project No. D2018-D000RC-0033.000)

e. ~~(S)~~ Recommendation 3.e. RUSSELL agrees with this recommendation. Navy (b)(1)(1.4g) [redacted]

f. (U/~~FOUO~~) Recommendation 4. RUSSELL agrees with this recommendation. Navy (b)(1)(1.7e) [redacted]

g. ~~(S)~~ Recommendation 6. RUSSELL agrees with this recommendation. Navy (b)(1)(1.4g) [redacted]

FOSTER.MATTH EW.W [redacted]

M. W. FOSTER

Derived from: DoD IG Memorandum dtd January 17, 2019
Declassify on: 20440219

Copy to:
CDS-23
CNSP
CPF
PMW 160

~~SECRET~~
2

# (U) Source of Classified Information

(U) The documents listed below are sources used to support classified information within this report.

**Source 1:** (U) USS *Abraham Lincoln* SIPRNet Vulnerability Scans (Document classified SECRET)
Declassification Date: August 31, 2043
Generated Date: August 31, 2018

**Source 2:** (U) USS *Ronald Reagan* SIPRNet Vulnerability Scans (Document classified SECRET)
Declassification Date: August 31, 2043
Generated Date: August 31, 2018

**Source 3:** (U) USS *Ramage* SIPRNet Vulnerability Scans (Document classified SECRET)
Declassification Date: August 31, 2043
Generated Date: August 31, 2018

**Source 4:** (U) USS *Russell* SIPRNet Vulnerability Scans (Document classified SECRET)
Declassification Date: August 31, 2043
Generated Date: August 31, 2018

**Source 5:** (U) E-mail From USS *Abraham Lincoln* Combat Systems Officer Regarding Mission Criticality of CANES (Document classified SECRET)
Declassification Date: July 27, 2043
Generated Date: July 27, 2018

# (U) Acronyms and Abbreviations

| | |
|---|---|
| **CANES** | Consolidated Afloat Networks and Enterprise Services |
| **CAT** | Category |
| **HBSS** | Host Based Security System |
| **NETWARCOM** | Naval Network Warfare Command |
| **NIPRNet** | Non-Classified Internet Protocol Router Network |
| **PMW 160** | Program Manager, Warfare 160: Tactical Networks |
| **SIPRNet** | Secret Internet Protocol Router Network |
| **SPAWAR** | Space and Naval Warfare Systems Command |
| **USS** | U.S. Ship |

# (U) Glossary

(U) **Antivirus.** A type of software used for scanning, detecting, and removing viruses from your computer.

(U) **Authentication.** A security measure designed to protect a communications system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission, message, originator, or a means of verifying an individual's eligibility to receive specific categories of information.

(U) **Availability.** Timely, reliable access to data and information services for authorized users.

(U) **Consolidated Afloat Networks and Enterprise System (CANES).** A commercial-off-the-shelf integration program designed to provide a complete network and enterprise services infrastructure comprising of commercial-off-the-shelf hardware, software, processing, storage, and end user devices for a wide variety of Naval ships. CANES operates in unclassified, secret, and top secret sensitive compartmented information enclaves, and provides all basic network services.

(U) **Category I (CAT I) Vulnerability.** If exploited by unauthorized users, could allow unauthorized personnel to bypass primary security protections and gain immediate network access.

(U) **Category II (CAT II) Vulnerability.** If exploited by unauthorized users, has the potential to result in unauthorized network access or activity.

(U) **Confidentiality.** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

(U) **Cross-Domain Solution.** The act of manually or automatically accessing or transferring information between different security domains.

(U) **Computer Network Defense Deployer Toolkit.** Defensive cyberspace operations tools used by Navy network defenders to identify network intrusions and collect network audit logs.

(U) **Data Integrity.** The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.

(U) **Enclaves.** A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter.

(U) **Host Based Security System (HBSS).** A set of capabilities that provide a framework to implement a wide-range of security solutions on hosts. This framework includes a trusted agent and a centralized management function that together provide automated protection to detect, respond, and report host based vulnerabilities and incident.

(U) **Intrusion Prevention Systems.** Security devices that detect unusual or malicious activities and attempt to stop detected possible incidents.

(U) **Malware.** Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms, of adware are also examples of malicious code.

(U) **Network Boundary Firewall.** Security devices that limit access between logical perimeters of a network.

(U) **Non-Repudiation.** Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

(U) **Plan of Action and Milestones**. A document that identifies tasks needing to be accomplished. It details a plan of action for vulnerability mitigation of organizational assets that cannot be patched, updated, or upgraded as mandated by U.S. Cyber Command orders and directives.

(U) **Removable Media.** Removable media are items such as compact discs, digital video disc, secure digital cards, tape, flash memory data storage devices, diskettes, multi-media cards, and external hard drives.

(U) **Routers.** Security devices that analyze the content of information transmitted within or between networks.

(U) **Switches.** Security devices that receive and redirect incoming network traffic to specific areas within the network.

(U) **Vulnerability.** Weakness in an information system, system security procedures, internal controls, or implementation that could exploited by a threat source.

(U) **Vulnerability Remediation Asset Manager.** Web-based network vulnerability data repository and analysis tool, which increases Navy cybersecurity awareness by providing visibility into system vulnerabilities.

(U) **Write Privilege.** Permissions granted to a user or device to transfer data to an object such as removable media.

## Whistleblower Protection

### U.S. Department of Defense

*Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible waste, fraud, and abuse in government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil*

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

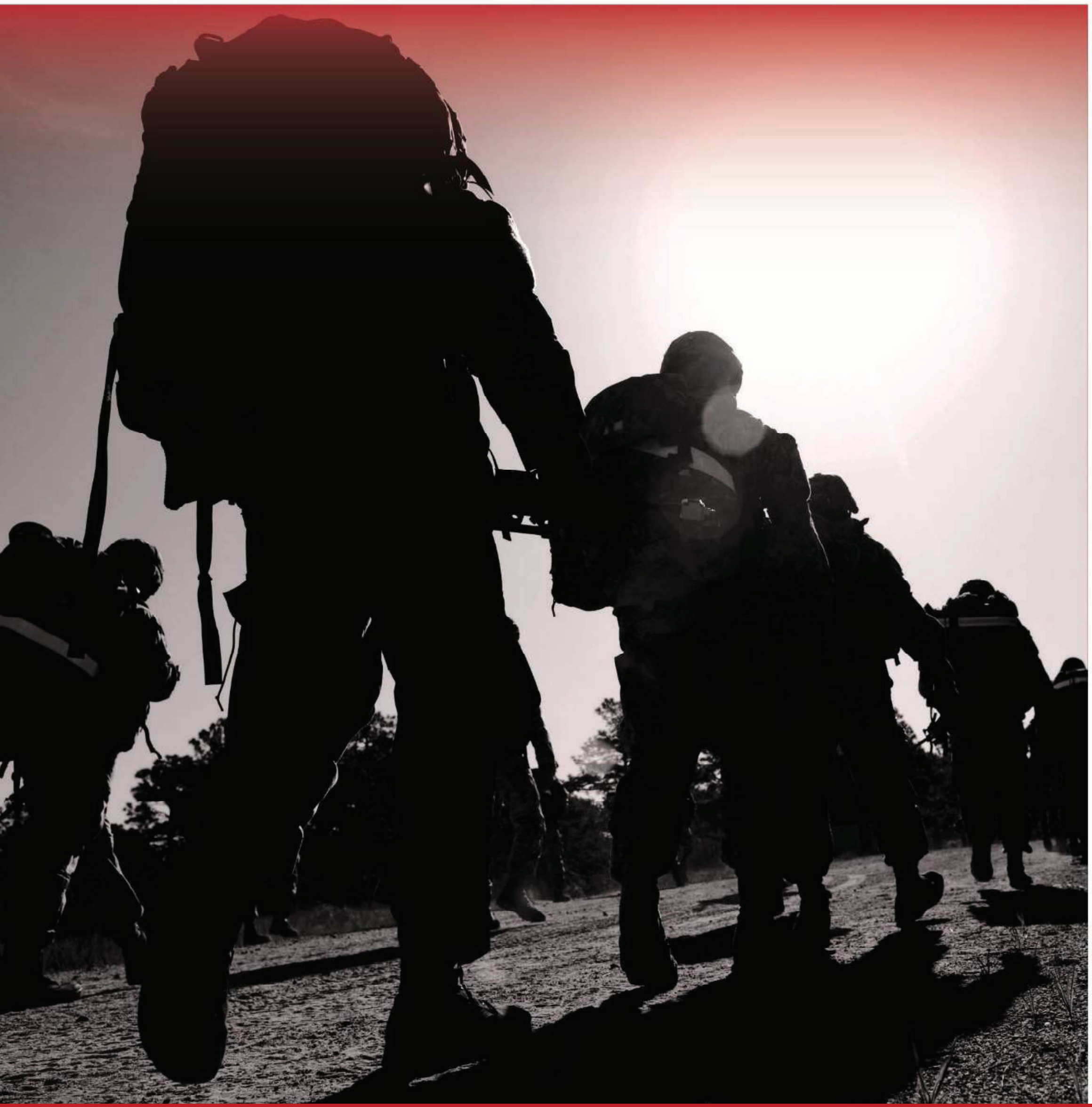
**Congressional Liaison**
703.604.8324

**Media Contact**
public.affairs@dodig.mil; 703.604.8324

**DoD OIG Mailing Lists**
www.dodig.mil/Mailing-Lists/

**Twitter**
www.twitter.com/DoD_IG

**DoD Hotline**
www.dodig.mil/hotline



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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