DoD OIG Report No: DODIG-2025-066
DHS OIG Report No: OIG-25-15

INSPECTORS GENERAL

*U.S. Department of Defense &*
*U.S. Department of Homeland Security*

# (U) Joint Audit of Security Controls over Coast Guard Systems Operating on the Department of Defense Information Network

FEBRUARY 7, 2025

~~Controlled by: DoD OIG / AUD~~
~~CUI Category: DCRIT, ISVI, OPSEC, PROPIN, PRVCY~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC: Program Director for Audit, Cyberspace Operations,~~ [redacted]

~~(CUI)~~ Compilation Notice: The compilation of unclassified information that reveals whether [redacted] is CUI by compilation.

INSPECTOR GENERAL
INTEGRITY EFFICIENCY
DEPARTMENT OF DEFENSE

U.S. DEPARTMENT OF HOMELAND SECURITY
OIG
INTEGRITY • ACCOUNTABILITY • EXCELLENCE
OFFICE OF INSPECTOR GENERAL

# (U) Results in Brief

## (U) Joint Audit of Security Controls over Coast Guard Systems Operating on the Department of Defense Information Network

February 7, 2025

## (U) Objective

(U) The objective of this joint audit was to determine whether the Coast Guard implemented cybersecurity controls to protect Coast Guard systems operating on the Department of Defense (DoD) Information Network (DODIN) in accordance with applicable cybersecurity requirements. The Coast Guard must comply with DoD cybersecurity requirements because its systems operate on the DODIN. The Coast Guard's roles and responsibilities for operating its systems on the DODIN are set forth in a series of memorandums between the DoD and the Department of Homeland Security (DHS).

## (U) Findings

(U) The Coast Guard did not consistently implement the cybersecurity controls we reviewed to protect its systems operating on the DODIN in accordance with applicable cybersecurity requirements. Specifically, for the three systems we reviewed, Coast Guard officials did not:

- (U) control logical access to privileged user accounts,
- (U) control or monitor physical access to server rooms,
- (U) develop contingency plans that included detailed recovery procedures or conduct annual plan reviews,
- (U) prepare plans of action and milestones for high and critical-severity vulnerabilities in a timely manner,
- ~~(CUI)~~ [redacted], or
- ~~(CUI)~~ [redacted].

## (U) Findings (cont'd)

(U) This occurred because Coast Guard officials followed Coast Guard policies, which did not always align with DoD requirements. The Assistant Commandant for Command, Control, Communications, Computer, and Information Technology/Coast Guard Chief Information Officer (CIO) also assigned only one information system security manager (ISSM) to provide oversight and monitor compliance with cybersecurity requirements for all Coast Guard systems instead of requiring system owners to designate an ISSM for each system as required by DoD guidance.

(U) In addition, the Commander, Coast Guard Cyber Command (CGCYBER) was not reissuing authorizations to operate every 3 years for the three systems we reviewed but continued to operate those systems and 35 other Coast Guard systems without authorizations to operate. The systems did not have authorizations to operate because the Assistant Commandant established an ongoing authorization program that was inconsistent with DoD requirements and without DoD CIO or DHS CIO approval.

(U) As a result, the three systems we reviewed, and other similarly situated systems in the Coast Guard's enterprise, are vulnerable to cybersecurity weaknesses and exposed to unassessed risks that could result in the unauthorized disclosure or compromise of sensitive Coast Guard information. Adversaries also could leverage these cybersecurity weaknesses to compromise the DODIN, placing DoD and Coast Guard personnel, assets, and the Nation at risk.

## (U) Recommendations

(U) Among 28 recommendations, we recommend that the DoD CIO develop and implement a process to ensure that the Coast Guard complies with DoD requirements for obtaining authorizations to operate systems on the DODIN. We also recommend that the Assistant Commandant update Coast Guard cybersecurity policies to align with DoD requirements and direct Coast Guard system owners to designate an ISSM for every Coast Guard system and that the CGCYBER Commander issue authorization decisions for the three systems we reviewed.

## (U) Management Comments and Our Response

(U) The Acting DoD CIO disagreed with developing and implementing a process to ensure that the Coast Guard complies with DoD requirements for obtaining authorizations to operate systems on the DODIN; therefore, the recommendation is unresolved. The Deputy Assistant Commandant for Resources, agreed with all 27 recommendations addressed to Coast Guard officials. Of those 27 recommendations, 21 are resolved but open, 4 are unresolved, and 2 are closed.

~~(CUI)~~ We request that the Acting DoD CIO; Assistant Commandant for Command, Control, Communications, Computer, and Information Technology/Chief Information Officer; CGCYBER Commander; [redacted]; and [redacted] provide additional comments within 30 days of the final report for the unresolved recommendations. Please see the Recommendations Table on the next page for the status of recommendations.

## (U) Recommendations Table

| ~~(CUI)~~<br>(U) Management | (U) Recommendations Unresolved | (U) Recommendations Resolved | (U) Recommendations Closed |
|---|---|---|---|
| (U) Chief Information Officer of the Department of Defense | 5 | None | None |
| (U) Assistant Commandant for Command, Control, Communications, Computer, and Information Technology/Chief Information Officer of the Coast Guard | 1.f | 1.a.1, 1.a.2, 1.a.3, 1.a.4, 1.a.5, 1.b.1, 1.b.2, 1.b.3, 1.b.4, 1.c.1, 1.c.2, 1.c.3, 1.c.4, 1.d, 1.e | None |
| (U) Commander, Coast Guard Cyber Command | 4.d | 4.a, 4.b, 4.c | 4.e |
| ~~(CUI)~~ [redacted] | 2.b | None | 2.a |
| ~~(CUI)~~ [redacted] | 3.c | 3.a, 3.b, 3.d | None<br>~~(CUI)~~ |

(U) Please provide Management Comments by March 10, 2025.

**(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** – The DoD OIG and DHS OIG verified that the agreed upon corrective actions were implemented.

INSPECTOR GENERAL
INTEGRITY EFFICIENCY
DEPARTMENT OF DEFENSE

U.S. DEPARTMENT OF HOMELAND SECURITY
OIG
INTEGRITY • ACCOUNTABILITY • EXCELLENCE
OFFICE OF INSPECTOR GENERAL

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

**INSPECTOR GENERAL**
**DEPARTMENT OF HOMELAND SECURITY**
245 MURRAY DRIVE SW
WASHINGTON, DC 20528-0305

February 7, 2025

MEMORANDUM FOR COMMANDANT OF THE COAST GUARD
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE

SUBJECT: (U) Joint Audit of Security Controls over Coast Guard Systems Operating on the Department of Defense Information Network (Report Nos. DODIG-2025-066 and OIG-25-15)

(U) This final report provides the results of the joint audit conducted by the DoD and DHS Offices of Inspector General. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

(U) This report contains five recommendations that we consider unresolved because the Acting DoD Chief Information Officer and the Deputy Assistant Commandant for Resources did not agree with or fully address the recommendations. We will track these recommendations until management officials have agreed to take actions that we determine to be sufficient to meet the intent of the recommendations and provide adequate documentation showing that all agreed-upon actions to implement the recommendations are completed.

(U) This report contains 21 recommendations that we consider resolved but open. We will close the recommendations when management provides documentation showing that all agreed-upon actions to implement the recommendations are completed.

(U) This report contains two recommendations that we consider closed because management took adequate action to fully address the recommendations.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. Therefore, please provide, within 30 days, your response concerning specific actions in process or alternative corrective actions proposed on the unresolved recommendations. In addition, please provide, within 90 days, your responses concerning specific actions in process or completed on the resolved recommendations. Send your responses to either [redacted] if unclassified or [redacted] if classified SECRET.

(U) We appreciate the cooperation and assistance received during the audit. If you have any questions, please contact Mr. Brett A. Mansfield, Deputy Inspector General for Audit, at [redacted] or Ms. Kristen D. Bernard, Deputy Inspector General for Audits, at [redacted].

Steven A. Stebbins

Steven A. Stebbins
Acting Inspector General
DoD Office of Inspector General

Joseph V. Cuffari

Joseph V. Cuffari, Ph.D
Inspector General
DHS Office of Inspector General

# (U) Contents

## (U) Introduction

## (U) Finding. The Coast Guard Did Not Consistently Implement Cybersecurity Controls to Protect Its Systems Operating on the DODIN 8

## (U) Appendix 38

## (U) Management Comments

## (U) Acronyms and Abbreviations 54

# (U) Introduction

## (U) Objective

(U) The objective of this joint audit was to determine whether the Coast Guard implemented cybersecurity controls to protect Coast Guard systems operating on the Department of Defense (DoD) Information Network (DODIN) in accordance with applicable cybersecurity requirements.[1] The Coast Guard must comply with DoD cybersecurity requirements because its systems operate on the DODIN. The Coast Guard's roles and responsibilities for operating its systems on the DODIN are set forth in a series of memorandums between the DoD and the Department of Homeland Security (DHS). See Appendix A for the scope and methodology and prior coverage related to the objective.

(U) Due to the magnitude of audit staff turnover since we announced the audit in May 2021, we conducted additional site visits and testing from April 2023 through August 2023. The results of those site visits and testing form the basis of the findings and recommendations of this report and therefore are relevant to the Coast Guard's existing operations.

## (U) Background

(U) The Coast Guard is one of the six U.S. Military Services. During peacetime, the Coast Guard operates as a component of the DHS to enforce the Nation's laws at sea and protect more than 100,000 miles of U.S. coastline, inland waterways, and ports. Upon a congressional declaration of war or the President's direction, the Coast Guard serves as a part of the Department of the Navy to support the DoD in combat and perform, among other missions, search and rescue, troop transport, and port security missions.

~~(CUI)~~ In support of its DoD mission, the Coast Guard was operating [redacted] information systems on the DODIN as of March 2024. The DODIN is the DoD's set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone. In January 2017, the Secretaries of Defense and Homeland Security signed a memorandum of agreement that defines the Coast Guard's roles and responsibilities for operating its systems

[1] (U) This report contains information that has been redacted because it was identified by the Department of Defense or Department of Homeland Security as Controlled Unclassified Information (CUI) or For Official Use Only (FOUO) information that is not releasable to the public. CUI and FOUO information are U.S. Government-created or owned unclassified information that allow for, or require, safeguarding and dissemination controls in accordance with laws, regulations, or U.S. Government-wide policies.

~~(CUI)~~ on the DODIN.[2] The memorandum requires, among other responsibilities, that the Coast Guard comply with DoD cybersecurity requirements for its systems operating on the DODIN, while continuing to comply with DHS guidance and oversight requirements for acquisitions, financial reporting, and the Federal Information Security Management Act reporting requirements.[3]

(U) In June 2019, the DHS Chief Information Officer (CIO) issued a memorandum to inform the Office of Management & Budget Federal CIO that the Coast Guard would manage its systems under the DoD's direction and fulfill its Federal Information Security Management Act reporting requirements through the DoD.[4] In May 2020, the DHS and Coast Guard CIOs issued a memorandum to the Acting Secretary of Homeland Security that reiterated the terms of the June 2019 memorandum and informed the Acting Secretary that because Coast Guard systems operated only on the DODIN, there was low risk to the DHS and all operational risk resided with the DoD.[5] In November 2023, the DHS CIO rescinded the authority for the Coast Guard to fulfill its Federal Information Security Management Act reporting requirements through the DoD and reiterated that the Coast Guard must continue complying with DoD cybersecurity requirements when operating on the DODIN.[6]

## *(U) DoD Cybersecurity Requirements*

(U) DoD Instruction 8500.01 establishes the DoD cybersecurity program.[7] The Instruction requires DoD Component Heads to develop Component-level cybersecurity programs, appoint authorizing officials for information systems, and operate only systems with an authorization to operate (ATO) in accordance with the Risk Management Framework (RMF).[8] An ATO is the official management decision made by an authorizing official to authorize operation of an information system and to explicitly accept the risk to agency operations and assets, individuals,

[2] (U) "Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations," January 19, 2017.

[3] (U) Before the January 2017 memorandum of agreement, the Coast Guard required that Coast Guard officials comply with DoD and DHS cybersecurity policies and apply the more stringent standards when the policies were different.

(U) The "Federal Information Security Management Act" requires Federal agencies to develop, document, and implement an agency-wide program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.

[4] (U) "United States Coast Guard Alignment to Department of Defense Cybersecurity," June 10, 2019.

[5] (U) "U.S. Coast Guard Cybersecurity Reporting," May 28, 2020.

[6] (U) "Rescission of Department of Homeland Security (DHS) Approval for U.S. Coast Guard Cybersecurity Reporting to Department of Defense (DoD)," November 13, 2023.

[7] (U) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014 (incorporating change 1, October 7, 2019).

[8] (U) The RMF is the U.S. Government's structured process for managing security and privacy risks for information systems.

(U) other organizations, and the Nation based on the implementation of an agreed-upon set of cybersecurity and privacy controls contained in the National Institute of Standards and Technology (NIST) Special Publication 800-53.[9]

(U) DoD Instruction 8510.01 requires DoD Components to implement the RMF and the DoD CIO's RMF guidance.[10] As part of the RMF process, a system owner must develop a system security plan that identifies the cybersecurity controls required to protect a system and the plan to implement the controls to meet DoD requirements.[11] In addition, system owners must obtain and renew their ATOs every 3 years.

(U) Chairman of the Joint Chiefs of Staff (CJCS) Instruction 6510.01F establishes joint cybersecurity policies and responsibilities for DoD Components.[12] Among other requirements, the CJCS Instruction requires DoD Components to implement the Defense Information Systems Agency's Security Technical Implementation Guides (STIG), which include cybersecurity control requirements for information systems.[13] In addition, the CJCS Instruction requires DoD Components to comply with U.S. Cyber Command (USCYBERCOM) directions, such as USCYBERCOM Tasking Orders.[14]

## *(U) Coast Guard Cybersecurity Policies and Procedures*

(U) Commandant Instruction 5500.13G is the Coast Guard's Component level cybersecurity guidance required by DoD Instruction 8500.01.[15] The Instruction establishes the Coast Guard cybersecurity program and contains policies and guidance for implementing cybersecurity controls for Coast Guard systems.

[9] (U) NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, April 30, 2013 (updated January 22, 2015).

(U) Cybersecurity controls are safeguards and countermeasures that are designed to protect the confidentiality, integrity, and availability of information that is processed by, stored on, and transmitted through DoD networks. Safeguards are protective measures and controls developed to meet the security requirements for a system. Countermeasures are actions, devices, procedures, techniques, or other measures that reduce vulnerabilities to a system.

[10] (U) DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022.

[11] (U) A system owner is the official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system.

[12] (U) CJCS Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011 (current as of June 9, 2015).

[13] (U) The Defense Information Systems Agency is a DoD agency responsible for developing cybersecurity guidance and processes to implement DoD cybersecurity policies.

[14] (U) USCYBERCOM is the Nation's unified combatant command for the cyberspace domain and is responsible to defend the DODIN, provide support to combatant commanders in the execution of their cyber missions around the world, and strengthen the Nation's ability to withstand and respond to cyber-attacks.

(U) USCYBERCOM issues Tasking Orders to task and disseminate cyberspace operations missions and targets to DoD Components.

[15] (U) Commandant Instruction 5500.13G, "U.S. Coast Guard Cybersecurity Policy," January 25, 2022.

(U) The Commandant Instruction also identifies the cybersecurity roles and responsibilities of Coast Guard officials. The Assistant Commandant for Command, Control, Communications, Computer, and Information Technology (designated with an additional title as Coast Guard CIO); Coast Guard Cyber Command (CGCYBER); and Command, Control, Communications, Computer, Cyber, and Intelligence Service Center (C5ISC), share the responsibility for implementing the Coast Guard's cybersecurity program.[16]

## *(U) Coast Guard Chief Information Officer*

(U) The Coast Guard CIO is responsible for the management and oversight of all Coast Guard information technology and cybersecurity. The Coast Guard CIO is required to appoint a Senior Information Security Officer (SISO) to direct and coordinate the Coast Guard cybersecurity program.[17] In addition, the Coast Guard CIO is also required to appoint authorizing officials and designate and provide instruction to Coast Guard system owners.

## *(U) Coast Guard Cyber Command*

(U) The CGCYBER Commander is the authorizing official for Coast Guard information systems, and the CGCYBER is the Coast Guard‘s Tier II cybersecurity service provider under the direction of USCYBERCOM.[18] CGCYBER officials are required to defend, monitor, and maintain the Coast Guard's network, including conducting cybersecurity inspections consistent with DoD standards. The CGCYBER information system security manager (ISSM) is required to develop, maintain, and oversee the implementation of system-specific cybersecurity programs for Coast Guard information systems.

(U) The CGCYBER security control assessors (SCA) are required to independently assess and issue security assessment reports on whether system owners properly implement security controls. In addition, CGCYBER Cybersecurity Operations Center officials monitor and respond to cyber incidents and network activity affecting all Coast Guard systems.[19]

[16] (U) Commandant Instruction 5401.5A, "Commandant (CG-6) Directorate and Associated Duties," May 6, 2014, establishes the roles and responsibilities of the Assistant Commandant for Command, Control, Communications, Computers, and Information Technology. For the purposes of this report, we refer to the Assistant Commandant as the Coast Guard CIO.

[17] (U) A SISO is responsible for developing, documenting, and implementing information security programs in compliance with section 3554, title 44, United States Code.

[18] (U) A Tier II cybersecurity service provider is an organization that USCYBERCOM has authorized to provide services, such as continuous monitoring and cyber incident handling, to protect a DoD Component on the DODIN.

[19] (U) Cyber incidents are actions or threats, such as network intrusions and suspicious emails, which result in an actual or potentially adverse effect on an information system.

## *(U) Command, Control, Communications, Computer, Cyber, and Intelligence Service Center*

(U) The C5ISC Commanding Officer is required to provide information technology to meet Coast Guard missions. The C5ISC information system security officers (ISSO) serve as cybersecurity leads for their assigned systems and enforce cybersecurity policies and prepare plans of action and milestones (POA&M) to address vulnerabilities with systems.[20] A POA&M identifies the actions and resources needed to remediate system vulnerabilities, the milestones to complete the actions, and any mitigations until the actions are fully implemented.

## *(U) Coast Guard Systems and Controls Reviewed*

~~(CUI)~~ To determine whether the Coast Guard implemented cybersecurity controls to protect Coast Guard systems operating on the DODIN, we reviewed the Coast Guard's implementation of cybersecurity controls for 3 [redacted] Coast Guard systems that were operating on the DODIN as of June 2021. We selected the three systems based on Coast Guard descriptions of the systems, CGCYBER assessments of the system risks, and input from DoD OIG information technology specialists.

- **~~(CUI)~~** [redacted].[21] [redacted].[22] [redacted]
- **~~(CUI)~~** [redacted].[23] [redacted]

[20] (U) Vulnerabilities are exploitable weaknesses in software or hardware that provide an adversary with an opportunity to compromise the confidentiality, integrity, or availability of an information system.

[21] (U) [redacted]

[22] (U) [redacted]

[23] (U) [redacted]

- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted].[24] [redacted]

(U) We focused our review on the following cybersecurity controls that we determined, if not implemented in accordance with DoD requirements, could present a high risk to the compromise of the information stored on the Coast Guard systems.

- **(U) Logical Access Controls**. Controls that prescribe who may access an information system and the type of account that they are authorized, such as a privileged user account.[25] We focused on controls over the privileged user accounts because they provide elevated, often unrestricted access to an organization's underlying information systems and technology, making them targets for both external and internal malicious actors.
- **(U) Physical Access Controls**. Controls that provide layered and complementary physical security to control and monitor access to facilities containing information system equipment, such as security guards, automated entry control systems, intrusion detection systems, and closed-circuit video monitors. We focused on controls over server rooms because servers store files, process data, and manage network traffic and are therefore primary targets for malicious actors.
- **(U) Contingency Plans**. Controls that require detailed plans and procedures to recover information systems after disruptive events that could cause information systems to be inoperable. A disruptive event is an unplanned event that causes an information system to be inoperable for a length of time. Disruptive events can result in a wide range of impacts, such as brief unavailability from a short-term power outage to long-term disablement from a natural disaster.

[24] (U) [redacted]

[25] (U) DoD Instruction 8500.01 identifies that a privileged user is authorized to have access to perform system control, monitoring, administration, or security-relevant functions that ordinary users are not authorized to perform.

- **(U) Vulnerability Management**. Controls that require the remediation of vulnerabilities in a timely manner and, if not, mitigations should be implemented and POA&Ms must be prepared. Remediation is the fix or neutralization of potential security risks and mitigation are temporary safeguards or countermeasures that reduce the risks from vulnerabilities until permanent corrective actions can be implemented to remediate the vulnerabilities. We focused on controls for high and critical-severity vulnerabilities because, if not remediated in a timely manner, these can result in catastrophic and cataclysmic adverse effects on DoD operations, assets, and individuals.
- **(U)** [redacted]
- **(U)** [redacted]

# (U) Finding

## (U) The Coast Guard Did Not Consistently Implement Cybersecurity Controls to Protect Its Systems Operating on the DODIN

~~(CUI)~~ The Coast Guard did not consistently implement the cybersecurity controls we reviewed to protect its systems operating on the DODIN in accordance with applicable cybersecurity requirements. Specifically, for the [redacted] [redacted] systems, Coast Guard officials did not:

- (U) control logical access to privileged user accounts,
- (U) control or monitor physical access to server rooms,
- (U) develop system contingency plans that included detailed recovery procedures or conduct annual plan reviews,
- (U) prepare POA&Ms for high and critical-severity vulnerabilities that are not remediated in a timely manner,
- ~~(CUI)~~ [redacted], or
- ~~(CUI)~~ [redacted].

(U) This occurred because Coast Guard officials followed Coast Guard policies and guidance, which did not always align with the corresponding DoD requirements. The Coast Guard CIO also assigned only one ISSM to provide oversight and monitor compliance with cybersecurity requirements for all Coast Guard systems instead of requiring system owners to designate an ISSM for each system as required by DoD guidance.

~~(CUI)~~ In addition to the inconsistent implementation of the controls we reviewed, the CGCYBER Commander was not reissuing ATOs every 3 years for the [redacted] systems but continued to operate those systems and 35 other Coast Guard systems without ATOs. The systems did not have ATOs because the Coast Guard CIO established an ongoing authorization program that was inconsistent with DoD requirements and without DoD CIO or DHS CIO approval.

~~(CUI)~~ As a result, the [redacted] systems, and other similarly situated systems in the Coast Guard's enterprise, are vulnerable to cybersecurity weaknesses and are exposed to unassessed risks that could result in the unauthorized disclosure or compromise of sensitive Coast Guard information,

~~(CUI)~~ including [redacted] records. This, in turn, could allow adversaries and malicious actors to [redacted]. Additionally, adversaries could also leverage these Coast Guard cybersecurity weaknesses to compromise the DODIN, placing DoD and Coast Guard personnel, assets, and the Nation at risk.

## (U) Coast Guard Officials Did Not Consistently Implement Security Controls

~~(CUI)~~ Coast Guard officials did not consistently implement security controls to protect its systems operating on the DODIN. Specifically, for the three systems we reviewed, Coast Guard officials did not control logical access to privileged user accounts; control or monitor physical access to server rooms; develop system contingency plans that included detailed recovery procedures or conduct annual plan reviews; prepare POA&Ms for high and critical-severity vulnerabilities in a timely manner; [redacted]; or [redacted].

### *(U) C5ISC ISSOs Did Not Control Logical Access to Privileged User Accounts*

~~(CUI)~~ The C5ISC ISSOs did not control logical access to privileged user accounts for the [redacted] systems. CJCS Instruction 6510.01F requires DoD Components to control access to information systems by ensuring all users have access agreements in place before granting logical access to the systems. The Traditional Security Checklist STIG requires each user to complete a DD Form 2875, or equivalent form, that includes a written justification for their access to a system and the approval of the system ISSO, or their appointee, to serve as the final official responsible for reviewing and approving the system access.[26] In addition, CJCS Instruction 6510.01F requires ISSOs to decide which accounts should be deleted when users no longer require access to their systems.

(U) To determine whether the C5ISC ISSOs controlled privileged user accounts in accordance with DoD cybersecurity requirements, we obtained and reviewed user lists for each system, identified the privileged users and their justification for privileged access to their respective systems, and verified whether the privileged users had DD Forms 2875 or equivalent forms for their privileged access that met DoD requirements.

[26] (U) "Traditional Security Checklist," STIG Version 2, Release 4, July 26, 2023.
(U) DD Form 2875, "System Authorization Access Request (SAAR)," May 2022. The DoD CIO designated the DD Form 2875 as the standard access agreement for DoD information systems.
(U) DoD Instruction 8500.01 states that ISSOs are responsible for ensuring that all users have system access authorizations before they are granted access to systems.

~~(CUI)~~ Of the [redacted] privileged users we identified, only 5 [redacted] privileged users had DD Forms 2875 or equivalent forms that met DoD requirements; the other [redacted] users did not. [redacted] The privileged user status by system is shown in Table 1.

*(U) Table 1. Privileged Users by System and Status*

| ~~(CUI)~~<br>(U) System | (U) Privileged Users with Access Forms | (U) Privileged Users Without Access Forms | ~~(CUI)~~ [redacted] | (U) Total Privileged Users |
|---|---|---|---|---|
| ~~(CUI)~~ [redacted] | (U) 0 | (U) 35 | ~~(CUI)~~ [redacted] | ~~(CUI)~~ [redacted] |
| ~~(CUI)~~ [redacted] | (U) 0 | (U) 41 | ~~(CUI)~~ [redacted] | ~~(CUI)~~ [redacted] |
| ~~(CUI)~~ [redacted] | (U) 5 | (U) 0 | ~~(CUI)~~ [redacted] | ~~(CUI)~~ [redacted] |
| **(U) Total** | **(U) 5** | **(U) 76** | ~~(CUI)~~ [redacted] | ~~(CUI)~~ [redacted]<br>~~(CUI)~~ |

(U) Source: The DoD OIG.

~~(CUI)~~ While reviewing the privileged user accounts, we identified 21 orphaned privileged user accounts, which had not been removed from the [redacted] servers.[27] An orphaned user account is an account that remains on computer hardware, such as a server, after the account has been deleted from a system. Orphaned user accounts represent ideal opportunities for malicious actors to gain access to a system because the accounts are not associated with active users. If a malicious actor gains control over an orphaned account with privileges, the malicious actor could access, traverse, and modify a network unnoticed. Therefore, the Coast Guard CIO should direct the [redacted] system owner to ensure that the ISSO identifies and removes all orphaned user accounts from the system.

~~(CUI)~~ Ineffective controls over the management of privileged user and other elevated accounts increase the risk that unauthorized individuals could compromise the cybersecurity of the [redacted] systems. According to National Security Telecommunications and Information Systems Security Advisory Memorandum 1-99, individuals with privileged user accounts pose the greatest threat to cybersecurity because they have the ability to make subtle and undetectable changes that can compromise a system.[28] [redacted]

[27] (U) [redacted]

(U) Privileges are special authorizations given to users to perform security relevant operations.

[28] (U) National Security Telecommunications and Information Systems Security Advisory Memorandum 1-99, "The Insider Threat to the Information Systems," July 1, 1999.

~~(CUI)~~ [redacted] Therefore, the Coast Guard CIO should direct the [redacted] system owners to ensure that the ISSOs identify all privileged users on their systems, obtain valid access agreements that justify the privileged users' continued access to the systems, and revoke the privileged user account of any user who does not provide an access agreement that justifies their privileged access.

## *(U) Coast Guard Security Personnel Did Not Control or Monitor Physical Access to All Server Rooms*

~~(CUI)~~ Coast Guard security personnel did not control or monitor physical access to the [redacted] server room and one of the [redacted] server rooms. CJCS Instruction 6510.01F requires commanders to establish physical security programs and plans to prevent and detect unauthorized physical access to facilities with information systems.[29] The Traditional Security Checklist STIG requires that the physical security plans specify layered and complementary security methods to control and monitor physical access to the facilities.[30]

~~(CUI)~~ To determine whether Coast Guard security personnel controlled and monitored physical access to the server rooms in accordance with DoD cybersecurity requirements, we obtained and reviewed physical security plans, inspected the server rooms, and compared physical access rosters with lists of badges from automated entry control systems. We reviewed one server room each for the [redacted] and [redacted] systems, and we reviewed two server rooms for the [redacted] system; one [redacted] server room supported a production environment and the other supported a test environment.[31]

~~(CUI)~~ Coast Guard security personnel controlled physical access to the [redacted] server room by maintaining a physical access roster and an automated entry control system with badge readers at each doorway to restrict access consistent with the roster. The Coast Guard security personnel also monitored access to the [redacted] server room with an intrusion detection system and closed-circuit video monitors.

[29] (U) CJCS Instruction 6510.01F requires commanders to establish physical security programs in accordance with DoD Regulation 5200.08, "Physical Security Program," April 9, 2007 (incorporating Change 2, October 19, 2020).

[30] (U) The Traditional Security Checklist STIG establishes requirements for physical security plans for facilities with information systems. The STIG identifies that security officials may use automated entry control systems, intrusion detection systems, closed-circuit video monitors, random guard patrols, or other safeguards to control physical access and detect, delay, assess, and respond to unauthorized access and other emergency situations.

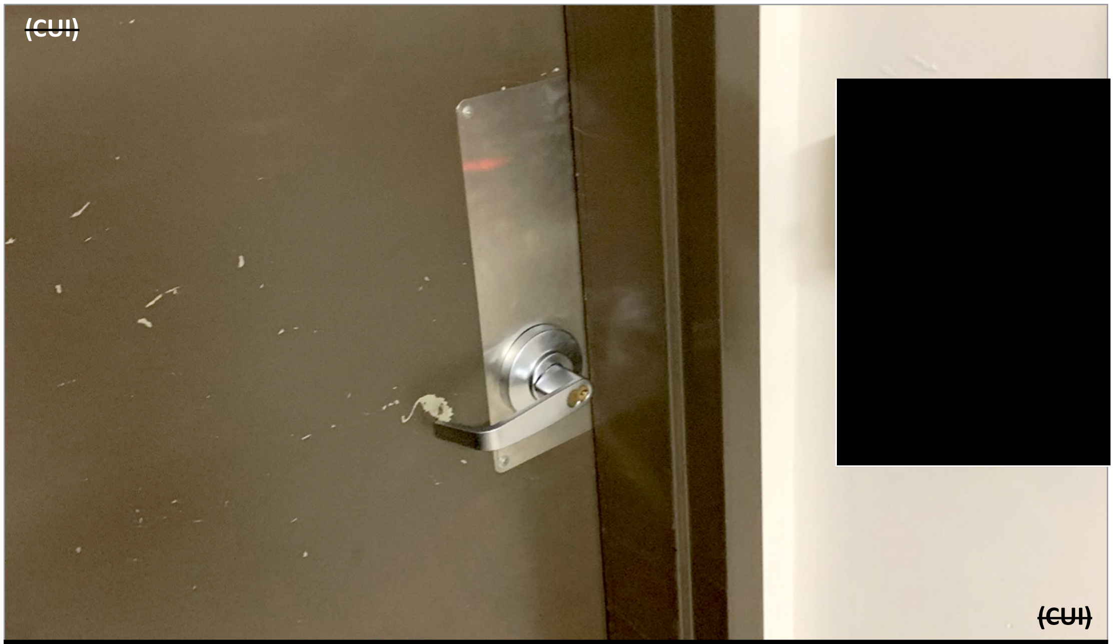
[31] (U) A production environment is the environment in which operations occur.

(U) A test environment should simulate the production environment as closely as possible but be separate so that system changes can be tested before installation in the production environment.

~~(CUI)~~ Coast Guard security personnel did not properly control physical access to the [redacted] server room. Although the security personnel maintained a physical access roster and an automated entry control system, the [redacted] server room had badge readers at only two of the four server room doors. At the two doors without badge readers, the security personnel relied on alternate security methods, such as latches, to prevent unauthorized access. However, the alternate security measures were not effective because there was no method to restrict access to approved personnel or to detect unauthorized access to the server room through those doors. Therefore, the [redacted] should implement controls to monitor physical access at all doors to the server room [redacted], in accordance with DoD physical security requirements for information technology.

~~(CUI)~~ Coast Guard security personnel controlled and monitored physical access to the [redacted] test environment server room but not the [redacted] production environment server room. Specifically, Coast Guard security personnel controlled physical access to the [redacted] test environment server room by maintaining a physical access roster and an automated entry control system with badge readers at the doorway to restrict access consistent with the roster. The Coast Guard security personnel also monitored access to the [redacted] test environment server room with an intrusion detection system and closed-circuit video monitors. However, for the [redacted] production environment server room, [redacted]. [redacted] officials stated that after our site visit, they discovered that the server room's automated entry control system was not operating properly and as a result, issued keys for a lever door lock so that supervisors could access the server room door and disabled the magnetic lock on the door.[32] Figure 1 is a picture of the lever door lock at the [redacted] production environment server room.

[32] ~~(CUI)~~ [redacted] officials were not using the lever door lock during our site visit because they were relying on the magnetic door lock.



~~(CUI)~~ Figure 1. Lever Door Lock at the [redacted] Production Environment Server Room
(U) Source: The DoD OIG.

~~(CUI)~~ According to the [redacted], they planned to protect the server room by installing a deadbolt lock on the door. However, a deadbolt lock would not provide layered and complementary physical security to control and monitor unauthorized physical access as required by the Traditional Security Checklist STIG. [redacted] officials also stated that there were random guard patrols that occurred across [redacted].[33] [redacted]. Therefore, the [redacted] should develop a physical access roster to identify the personnel authorized to access the [redacted] production environment server room, develop and implement procedures to update, when appropriate, the physical access roster, and develop and implement physical security methods to control and monitor physical access in accordance with DoD physical security requirements for information technology.

[33] ~~(FOUO)~~ [redacted]

~~(CUI)~~ [redacted]

## *(U) C5ISC ISSOs Did Not Develop Contingency Plans with Detailed Recovery Procedures or Conduct Annual Plan Reviews*

~~(CUI)~~ The C5ISC ISSOs did not develop contingency plans with detailed recovery procedures to restore the [redacted] systems after a disruptive event or conduct annual plan reviews. NIST Special Publication 800-34 states that contingency plans should include detailed recovery procedures to restore essential system functions and identify the roles, responsibilities, and contact information of officials responsible for implementing the procedures.[34] The DoD CIO requires ISSOs to annually review and approve contingency plans.

(U) To determine whether the ISSOs developed contingency plans with specific recovery procedures; identified the roles, responsibilities, and contact information of officials responsible for implementing these procedures; and reviewed the plans annually, we reviewed the contingency plans and interviewed the ISSOs. We also reviewed the contingency plan issuance dates to determine whether the ISSOs reviewed and approved the contingency plans annually.

~~(CUI)~~ The ISSOs did not include detailed procedures to recover the essential functions of the three systems in the contingency plans. For example, the [redacted] contingency plan required that the system administrators verify that the [redacted] system was "operational and functioning properly" once the recovery procedures were implemented but did not include detailed procedures on how to restore the system. Instead, the [redacted] system's procedures were available on [redacted] that could be unavailable during a disruptive event. The [redacted] contingency plan included recovery procedures that focused on topics unrelated to the essential functions of the system, such as preparing emergency supply kits and securing lodging.[35] Similarly, the [redacted] contingency plan included a recovery procedure to "test all [redacted] applications, components, services, network connections, database logs, and data feeds for operations ready" but did not detail

[34] (U) NIST Special Publication 800-34, "Contingency Planning Guide for Federal Information Systems," May 31, 2010 (updated November 11, 2010). DoD Instruction 8500.01 requires DoD Components to develop contingency plans for information systems in accordance with the Special Publication.

[35] (U) An emergency supply kit is a collection of basic items, such as medications and clothing, which an individual maintains so that they are prepared to quickly travel in response to an emergency.

~~(CUI)~~ how to perform the tests. In addition, none of the contingency plans identified the roles, responsibilities, or contact information of all officials responsible for implementing the plans.

~~(CUI)~~ The ISSOs also did not review or approve the contingency plans annually. The [redacted] contingency plans were not updated since June 2017, July 2021, and January 2020, respectively. Furthermore, none of the contingency plans were signed by the ISSOs to indicate approval.

~~(CUI)~~ Without up to date and detailed contingency plans, the Coast Guard may not be able to recover the [redacted] systems to perform essential functions necessary to successfully execute DoD and DHS missions. Therefore, the Coast Guard CIO should direct the [redacted] system owners to ensure that the ISSOs update and approve the contingency plans to ensure they include detailed recovery procedures and identify the officials responsible for implementing the procedures for the systems.

## *(U) C5ISC ISSOs Did Not Prepare POA&Ms for High and Critical-Severity Vulnerabilities in a Timely Manner*

~~(CUI)~~ The C5ISC ISSOs did not prepare POA&Ms for high and critical-severity vulnerabilities for the [redacted] systems in a timely manner. [redacted].[36] [redacted].[37] [redacted].

~~(CUI)~~ To determine whether the C5ISC ISSOs prepared POA&Ms for high and critical-severity vulnerabilities [redacted], we selected and reviewed a nonstatistical sample of 30 high or critical-severity vulnerabilities for the [redacted] systems between February and May 2023.[38] [redacted] we requested the POA&Ms for each of the vulnerabilities.

[36] ~~(CUI)~~ [redacted]

[37] (U) CJCS Manual 6510.02, "Information Assurance Vulnerability Management (IAVM) Program," November 5, 2013.

[38] ~~(CUI)~~ We obtained and compared [redacted] system vulnerability scans to identify vulnerabilities [redacted] which the scans categorized as high or critical-severity vulnerabilities. [redacted] We nonstatistically selected 10 vulnerabilities from each system. Nonstatistical sample results cannot be projected to an entire population.

~~(CUI)~~ The ISSOs were unable to provide POA&Ms for any of the vulnerabilities. For example, a scan of the [redacted] system on April 5, 2023, identified outdated software, which met the definition of a high-severity vulnerability. However, according to the ISSO, [redacted] the ISSO never developed a POA&M for the vulnerability. [redacted] In addition, there were several missing updates for servers across all three systems [redacted].

~~(CUI)~~ ISSOs develop POA&Ms to inform authorizing officials of the identified vulnerabilities and the resources, timelines, and actions that are required to remediate the vulnerabilities. Without POA&Ms, the CGCYBER Commander and other senior Coast Guard cybersecurity officials lacked visibility into the risks from unremediated vulnerabilities and how those risks could impact Coast Guard systems and the DODIN. Furthermore, the DHS's Cybersecurity Infrastructure and Security Agency identified that adversaries have previously exploited 3 of 30 vulnerabilities we reviewed and may be able to cause immediate damage to systems containing the vulnerabilities and increase the risk to the DODIN.[39] The ISSOs remediated all 30 vulnerabilities that we reviewed during the audit; however, there may still be other high and critical-severity vulnerabilities [redacted] for these systems. Therefore, the Coast Guard CIO should direct the [redacted] system owners to ensure that the ISSOs identify any high and critical-severity vulnerabilities [redacted] and prepare POA&Ms for those vulnerabilities.

~~(CUI)~~ During the audit, we issued a classified notice of concern to alert the USCYBERCOM Commander about a critical-severity vulnerability on the [redacted] system.[40] In response, the CGCYBER Deputy Commander provided records that demonstrated the [redacted] ISSO took corrective actions that fully addressed the vulnerability. Therefore, no further actions are necessary to address the notice of concern.

[39] (U) We verified that 3 of 30 vulnerabilities were included in the Cybersecurity Infrastructure and Security Agency's Known Exploited Vulnerabilities Catalog, which is an authoritative list of vulnerabilities that malicious cyber actors actively exploit to attack public and private organizations. The Cybersecurity Infrastructure Security Agency considers these vulnerabilities to be significant risks to Federal information systems and requires Federal civilian agencies to aggressively remediate these vulnerabilities to reduce cyber incidents.

[40] (U) DoD OIG, "Notice of Concern on Joint Audit of Security Controls Over Coast Guard Systems Used and Operated on the DoD Information Network," September 30, 2022. To request a copy of the classified notice of concern, please review the DoD OIG Freedom of Information Act Office instructions at https://www.dodig.mil/FOIA/.

***~~(CUI)~~*** [redacted]

~~(CUI)~~ [redacted].[41] [redacted]

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]

[41] ~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted].[42] [redacted]

- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]

### ***~~(CUI)~~*** [redacted]

~~(CUI)~~ [redacted].[43]

[42] ~~(CUI)~~ [redacted]

[43] (U) [redacted]

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted].[44] [redacted]

## (U) Coast Guard Cybersecurity Policies and Guidance Did Not Always Align with DoD Requirements

~~(CUI)~~ The Coast Guard did not consistently implement cybersecurity controls for the [redacted] systems because the Coast Guard's cybersecurity policies and guidance did not always align with DoD requirements. The January 2017 memorandum of agreement between the Secretaries of Defense and Homeland Security requires that the Coast Guard comply with DoD cybersecurity requirements. The Coast Guard may issue more restrictive policies and guidance, but must, at a minimum, meet all DoD requirements. See Table 2 for a summary of differences between the DoD requirements and Coast Guard cybersecurity policies and guidance for controls we reviewed.

[44] ~~(CUI)~~ [redacted]

*(U) Table 2. Differences Between DoD Requirements and Coast Guard Policies or Guidance*

| ~~(CUI)~~<br>(U) Cybersecurity Control | (U) DoD Requirement | (U) Difference in Coast Guard Policy or Guidance |
|---|---|---|
| (U) Logical Access Controls | (U) DoD Instruction 8500.01 requires ISSOs (the DoD designated role assigned responsibility for maintaining the appropriate operational security posture for a system) to ensure that all users, including privileged users, have authorization for system access before the users are granted access, and CJCS Instruction 6510.01F requires each user to have an access agreement, such as a DD Form 2875, for each system accessed. ISSOs, or their appointees, are the final officials responsible for reviewing and approving access to a system. | ~~(FOUO)~~ [redacted] |
| (U) Physical Access Controls | (U) CJCS Instruction 6510.01F requires DoD Components to protect systems against unauthorized physical access. The Traditional Security Checklist STIG requires layered and complementary physical security methods, such as intrusion detection systems, closed-circuit video monitors, random guard patrols, or other safeguards, to control and monitor physical access to rooms containing system components such as servers. | ~~(FOUO)~~ [redacted][1] |
| (U) Vulnerability Management | ~~(CUI)~~ [redacted] | ~~(CUI)~~ The Coast Guard has two conflicting policies for POA&Ms for high and critical-severity vulnerabilities, [redacted].<br>~~(FOUO)~~ [redacted]<br>~~(CUI)~~ [redacted].[2]<br>~~(CUI)~~ |

*(U) Table 2. Differences Between DoD Requirements and Coast Guard Policies or Guidance (cont'd)*

| ~~(CUI)~~<br>(U) Cybersecurity Control | (U) DoD Requirement | (U) Difference in Coast Guard Policy or Guidance |
|---|---|---|
| (U) [redacted] | ~~(CUI)~~ [redacted] | ~~(FOUO)~~ [redacted]<br>~~(CUI)~~ |

[1] (U) Commandant Instruction Manual 5530.1C, "Physical Security and Force Protection Program," December 17, 2001 (incorporating Change 2, August 10, 2016).

[2] ~~(CUI)~~ [redacted]

(U) Source: The DoD OIG.

~~(CUI)~~ In January 2020, the Coast Guard CIO updated Commandant Instruction 5500.13 with the intention of aligning Coast Guard cybersecurity policies with DoD requirements. However, the Coast Guard SISO stated that the Coast Guard did not perform a comprehensive review of the cybersecurity policies and guidance and instead performed limited updates to the sections of the Commandant Instruction that were primarily based on DHS guidance. Therefore, to ensure Coast Guard cybersecurity policies and guidance align with DoD requirements, the Coast Guard CIO should review and crosswalk, in coordination with the DoD CIO, Coast Guard cybersecurity policies and guidance against DoD requirements, identify any instances in which Coast Guard policies or guidance are less restrictive or do not align with DoD requirements, and update the Coast Guard policies and guidance for those instances. At a minimum, the Coast Guard CIO should update the policies and guidance for logical access controls, physical access controls, vulnerability management, and [redacted].

## (U) The Coast Guard Did Not Provide Adequate Oversight or Monitor Compliance with Cybersecurity Requirements

~~(CUI)~~ The Coast Guard did not provide adequate oversight or monitor compliance with cybersecurity requirements for the [redacted] systems. Specifically, the Coast Guard CIO assigned a CGCYBER official to serve as the only ISSM to provide oversight and monitor compliance with cybersecurity requirements for all Coast Guard systems that process information up to the Secret level instead of requiring system owners to designate an ISSM for each system, as required by DoD guidance. DoD Instruction 8510.01 requires system owners to appoint an ISSM for each system. ISSMs are responsible for developing, maintaining, and implementing system-specific cybersecurity programs, including system-specific cybersecurity policies and procedures. In addition, ISSMs are responsible for monitoring compliance with cybersecurity policies and providing direction and oversight to ISSOs.

~~(CUI)~~ The ISSM stated that they had served in that role as a collateral duty for many years, but they did not have time to oversee the ISSOs or cybersecurity programs for many of the Coast Guard information systems. The ISSM added that to address this lack of oversight, the CGCYBER SCAs were unofficially performing ISSM duties.[45] This kept the SCAs from performing their primary responsibilities, which were to conduct independent, annual security control assessments for Coast Guard systems and document the results in security assessment reports. The DoD CIO authorizes each DoD Component to establish the baseline frequency at which its SCAs assess each control, and therefore the SCAs should have assessed each control at similar frequencies for every Coast Guard system.[46] However, the CGCYBER SCAs assessed 20.4 percent, 37.5 percent, and 1.5 percent of all cybersecurity controls for the [redacted] systems, respectively, during FY 2022 and FY 2023. In addition, the CGCYBER SCAs had not prepared security assessment reports for the [redacted] systems since 2018. Furthermore, because the SCAs unofficially performed ISSM duties, they had conflicts of interest that threatened their independence for the systems they assessed. To ensure that the Coast Guard provides adequate oversight of its cybersecurity program, the Coast Guard CIO should direct the Coast Guard system owners to designate an ISSM for every Coast Guard information system.

[45] (U) The ISSM and SCAs were assigned to separate departments in the CGCYBER, and the ISSM did not supervise the SCAs.

[46] (U) The frequencies may not be identical for every system because SCAs can tailor their assessments based on system-specific risks and due to timing differences across SCA assessments.

~~(CUI)~~ In addition, the CGCYBER Commander should direct the SCAs to conduct and document the results of annual security assessments in accordance with established control assessment frequencies for Coast Guard information systems and ensure that the SCAs are independent of the systems that they assess.

## (U) The Coast Guard Was Not Reissuing ATOs Every 3 Years

~~(CUI)~~ The CGCYBER Commander was not reissuing ATOs every 3 years for the [redacted] systems but continued to operate those systems and 35 other Coast Guard systems without ATOs. DoD Instruction 8510.01 states that only systems with current ATOs may operate on the DODIN, and the DoD CIO requires authorizing officials to reissue ATOs at least every 3 years to continue operating systems on the DODIN.

~~(CUI)~~ The most recent security authorization packages for the [redacted] [redacted] systems identified that the CGCYBER Commander had not reissued ATOs for the systems since 2018 and that the Commander "vacated" the durations of the ATOs instead of reissuing ATOs for the systems in 2021. CGCYBER officials stated that they did not need to reissue ATOs for the [redacted] [redacted] Coast Guard systems every 3 years because the CGCYBER Commander approved ongoing authorizations for the systems.[47] According to Commandant Instruction 5500.5A, the Coast Guard CIO established an Ongoing Authorization Program in June 2019, [redacted] [redacted].[48] CGCYBER officials stated that the Ongoing Authorization Program was intended to improve cybersecurity by allowing ISSOs to focus on risks rather than regularly updating security authorization packages to obtain ATOs.

~~(CUI)~~ According to Coast Guard CIO and CGCYBER officials, the Coast Guard did not seek DoD CIO or DHS CIO approval before establishing the Coast Guard Ongoing Authorization Program. The Coast Guard CIO stated that they were aware that the DoD did not have an ongoing authorization program, so they established the Coast Guard program based on an existing DHS program.[49] Although the DoD CIO established a similar program in February 2022, referred to as continuous ATO, an authorizing official must demonstrate to the Deputy DoD CIO for Cybersecurity

[47] (U) According to NIST Special Publication 800-37, "Risk Management Framework for Information Systems and Organizations," December 20, 2018, ongoing authorization is a process that provides near real-time information about system security to an authorizing official for a decision on whether to continue operating the system, considering mission requirements and risk tolerance. Ongoing authorization relies on a robust continuous monitoring program that enables the organization to monitor cybersecurity controls, verify the controls are operating as intended, and identify risks.

[48] (U) Commandant Instruction 5500.5A, "United States Coast Guard Ongoing Authorization (OA) Policy," January 21, 2022. The Coast Guard CIO issued the initial Commandant Instruction 5500.5 on June 7, 2019.

[49] (U) "Department of Homeland Security Ongoing Authorization Methodology," September 9, 2016.

~~(CUI)~~ that their DoD Component conducts robust continuous monitoring of cybersecurity controls, deploys active cyber defenses in response to cyber threats, and implements Development, Security, and Operations software engineering practices for a system.[50] The Coast Guard had not demonstrated their program to the Deputy DoD CIO, and the Coast Guard's Ongoing Authorization Program does not meet all of the DoD requirements for continuous ATOs [redacted]. To ensure that the Coast Guard complies with DoD ATO requirements, the Coast Guard CIO should rescind the Ongoing Authorization Program policy and update Coast Guard cybersecurity policy to require Coast Guard authorizing officials to issue ATOs at least every 3 years. If the Coast Guard intends to establish a program for continuous ATOs, the Coast Guard CIO should comply with the DoD CIO's approval process. In addition, the CGCYBER Commander should issue authorization decisions for all Coast Guard systems operating under Coast Guard Ongoing Authorization, including the [redacted] systems. The DoD CIO should develop and implement a process to ensure that the Coast Guard complies with DoD requirements for obtaining ATOs for information systems operating on the DODIN.

## (U) U.S. Adversaries and Malicious Actors Could Compromise Coast Guard and DoD Information

~~(CUI)~~ Without adequate cybersecurity controls and programs, the [redacted] systems, as well as other similarly situated systems in the Coast Guard's enterprise, are vulnerable to cybersecurity weaknesses and unassessed risks. Compromise of those cybersecurity weaknesses could result in the unauthorized disclosure or compromise of sensitive Coast Guard information, including [redacted] records. This, in turn, could allow adversaries and malicious actors to [redacted]. Additionally, adversaries could also leverage the Coast Guard cybersecurity weaknesses to compromise the DODIN, placing DoD and Coast Guard personnel, assets, and the Nation at risk.

## (U) Management Actions Taken

~~(CUI)~~ In response to the audit, the CGCYBER Commander issued ATOs for the [redacted] systems and other systems operating under the Coast Guard Ongoing Authorization Program. The Coast Guard CIO stated that they were not aware that the DoD CIO required authorizing officials to reissue ATOs at least every 3 years to continue operating systems on the DODIN.

[50] (U) Development, Security, and Operations software engineering practices are intended to automate, monitor, and apply security during all phases of the software development lifecycle.

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

(U) Although not required, the Deputy Assistant Commandant for Resources provided comments on the Finding. For the full text of the Deputy Assistant Commandant's comments, see the Management Comments section of the report.

### *(U) Deputy Assistant Commandant for Resources Comments*

(U) The Deputy Assistant Commandant for Resources expressed appreciation for the DoD and DHS OIGs' recognition that Coast Guard officials followed Coast Guard cybersecurity policies and guidance to protect their systems operating on the DODIN. In addition, the Deputy Assistant Commandant provided technical comments to address accuracy, contextual, and other issues with the report.

### *(U) Our Response*

(U) Although we acknowledge in this report that Coast Guard officials were following Coast Guard cybersecurity policies and guidance, the Coast Guard policies and guidance did not always align with the corresponding DoD requirements and, therefore, were not adequate to ensure that Coast Guard systems operating on the DODIN were protected. The Deputy Assistant Commandant's technical comments focused on security markings and the handling of Coast Guard information in this report, which we considered when applying portion markings and redactions.

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

### *(U) Revised Recommendation*

(U) As a result of management comments, we revised draft Recommendation 4.d to clarify that the CGCYBER Commander should direct the SCAs to conduct and document the results of annual security assessments on the controls assessed in accordance with the frequencies established by the Coast Guard.

### *(U) Recommendation 1*

**(U) We recommend that the Assistant Commandant for Command, Control, Communications, Computer, and Information Technology:**

a. **~~(CUI)~~ Direct the System Owner for the [redacted] system to ensure that the information system security officer:**

   1. **(U) Identifies and removes all orphaned user accounts from the system.**

2. **(U) Identifies all privileged users on their system and obtains valid access agreements that justify the privileged users' continued access to the system.**
3. **(U) Revokes the privileged user account of any user who does not provide an access agreement that justifies their privileged access.**
4. **(U) Updates and approves the contingency plan to ensure it includes detailed recovery procedures and identifies the officials responsible for implementing the procedures.**
5. **~~(CUI)~~ Identifies any high and critical-severity vulnerabilities [redacted] and prepares plans of action and milestones for those vulnerabilities.**

**b. ~~(CUI)~~ Direct the System Owner for the [redacted] system to ensure that the information system security officer:**

1. **(U) Identifies all privileged users on their system and obtains valid access agreements that justify the privileged users' continued access to the system.**
2. **(U) Revokes the privileged user account of any user who does not provide an access agreement that justifies their privileged access.**
3. **(U) Updates and approves the contingency plan to ensure it includes detailed recovery procedures and identifies the officials responsible for implementing the procedures.**
4. **~~(CUI)~~ Identifies any high and critical-severity vulnerabilities [redacted] and prepares plans of action and milestones for those vulnerabilities.**

**c. ~~(CUI)~~ Direct the System Owner for the [redacted] system to ensure that the information system security officer:**

1. **(U) Identifies all privileged users on their system and obtains valid access agreements that justify the privileged users' continued access to the system.**
2. **(U) Revokes the privileged user account of any user who does not provide an access agreement that justifies their privileged access.**

3. **(U) Updates and approves the contingency plan to ensure it includes detailed recovery procedures and identifies the officials responsible for implementing the procedures.**
4. **~~(CUI)~~ Identifies any high and critical-severity vulnerabilities [redacted] and prepares plans of action and milestones for those vulnerabilities.**

## *(U) Assistant Commandant for Command, Control, Communications, Computer, and Information Technology/Coast Guard Chief Information Officer Comments*

~~(CUI)~~ The Deputy Assistant Commandant for Resources, responding for the Coast Guard CIO, agreed, stating that the Coast Guard SISO would implement all of the recommendations.[51] Specifically, the Coast Guard SISO would identify and remove all orphaned privileged user accounts, identify all privileged users and obtain valid access agreements, revoke privileged user accounts for users without access agreements, complete contingency plans that identify detailed recovery procedures and responsible officials, and prepare POA&Ms for high and critical-severity vulnerabilities [redacted] for the [redacted] systems.[52] The Deputy Assistant Commandant expected that the Coast Guard SISO would complete these actions by December 31, 2024.

## *(U) Our Response*

~~(CUI)~~ Comments from the Deputy Assistant Commandant addressed all specifics of the recommendations; therefore, the recommendations are resolved but open. We will close the recommendations once the Coast Guard CIO provides:

- (U) a list of all privileged users and copies of their account access agreements that meet DoD requirements,
- (U) records that demonstrate there are no orphaned privileged user accounts,
- (U) approved contingency plans that include detailed recovery procedures and responsible officials, and
- ~~(CUI)~~ vulnerability scans with corresponding POA&Ms for any high and critical-severity vulnerabilities [redacted] for the [redacted] systems.

[51] (U) The Assistant Commandant for Command, Control, Communications, Computer, and Information Technology is designated with an additional title as the Coast Guard CIO. For the purposes of this report, we refer to the Assistant Commandant as the Coast Guard CIO.

[52] (U) The Coast Guard SISO is responsible for the Coast Guard's Office of Cybersecurity Program Management.

d. **~~(CUI)~~ Review and crosswalk, in coordination with the Department of Defense Chief Information Officer, Coast Guard cybersecurity policies and guidance against Department of Defense requirements, identify any instances in which the Coast Guard policies or guidance are less restrictive or do not align with Department of Defense requirements, and update the Coast Guard policies and guidance for those instances. At a minimum, update the policies and guidance for logical access controls, physical access controls, vulnerability management, and [redacted].**

### *(U) Assistant Commandant for Command, Control, Communications, Computer, and Information Technology/Coast Guard Chief Information Officer Comments*

(U) The Deputy Assistant Commandant for Resources, responding for the Coast Guard CIO, agreed, stating that the Coast Guard SISO would complete a review to identify Coast Guard policies that were less restrictive or did not align with DoD requirements and would update the policies, as appropriate. The Deputy Assistant Commandant expected that the Coast Guard SISO would complete these actions by June 30, 2025.

### *(U) Our Response*

~~(CUI)~~ Comments from the Deputy Assistant Commandant addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Coast Guard CIO provides the updated Coast Guard policies that, at a minimum, address logical access controls, physical access controls, vulnerability management, and [redacted].

e. **(U) Direct the Coast Guard system owners to designate an information system security manager for every Coast Guard information system.**

### *(U) Assistant Commandant for Command, Control, Communications, Computer, and Information Technology/Coast Guard Chief Information Officer Comments*

(U) The Deputy Assistant Commandant for Resources, responding for the Coast Guard CIO, agreed, stating that the Coast Guard SISO would identify an ISSM for each Coast Guard system. The Deputy Assistant Commandant expected that the Coast Guard SISO would complete these actions by March 31, 2025.

## *(U) Our Response*

~~(CUI)~~ Comments from the Deputy Assistant Commandant addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Coast Guard CIO provides the designation letters for the ISSMs assigned to the [redacted] systems and a list of ISSMs assigned to all Coast Guard systems operating on the DODIN.

f. **(U) Rescind the Ongoing Authorization Program policy and update Coast Guard cybersecurity policy to require Coast Guard authorizing officials to issue authorizations to operate at least every 3 years. If the Coast Guard intends to establish a program for continuous authorizations to operate, the Assistant Commandant should comply with the Department of Defense Chief Information Officer's approval process.**

## *(U) Assistant Commandant for Command, Control, Communications, Computer, and Information Technology/Coast Guard Chief Information Officer Comments*

(U) The Deputy Assistant Commandant for Resources, responding for the Coast Guard CIO, agreed, stating that the Coast Guard SISO would update Coast Guard cybersecurity policies to require authorizing officials to issue ATOs at least every 3 years. The Deputy Assistant Commandant expected that the Coast Guard SISO would complete these actions by June 30, 2025.

## *(U) Our Response*

(U) Comments from the Deputy Assistant Commandant partially addressed the recommendation; therefore, the recommendation is unresolved. Although the Deputy Assistant Commandant stated that the Coast Guard SISO will update cybersecurity policies to require ATOs at least every 3 years, the Deputy Assistant Commandant did not state that the Coast Guard CIO would rescind the Coast Guard's Ongoing Authorization Program policy. Therefore, we request that the Coast Guard CIO, within 30 days of the final report, provide additional comments on rescinding the Ongoing Authorization Program policy.

## (U) Recommendation 2

**~~(CUI)~~ We recommend that the [redacted]:**

a. **~~(CUI)~~ Implement controls to monitor physical access at all doors to the server room [redacted], in accordance with Department of Defense physical security requirements for information technology.**

### ~~(CUI)~~ [redacted] Comments

~~(CUI)~~ The Deputy Assistant Commandant for Resources, responding for the [redacted], agreed, stating that the [redacted] would implement controls to monitor physical access to all server room doors [redacted]. The Deputy Assistant Commandant expected that the [redacted] would complete these actions by September 30, 2025.

### (U) Our Response

~~(CUI)~~ Comments from the Deputy Assistant Commandant addressed all specifics of the recommendation. In addition, the [redacted] Chief of Security provided evidence that security personnel completed security upgrades that allowed them to monitor all the server room doors in the [redacted]. Therefore, this recommendation is closed.

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

### (U) Management Comments Required

~~(CUI)~~ The Deputy Assistant Commandant for Resources, responding for the [redacted] did not address the recommendation; therefore, the recommendation is unresolved. We request that the [redacted] provide comments, within 30 days of the final report, describing how they will [redacted].

## (U) Recommendation 3

**~~(CUI)~~ We recommend that the [redacted]:**

a. **~~(CUI)~~ Develop a physical access roster to identify the personnel authorized to access the [redacted] production environment server room at [redacted].**

### *~~(CUI)~~ [redacted] Comments*

~~(CUI)~~ The Deputy Assistant Commandant for Resources, responding for the [redacted], agreed, stating that the [redacted] developed a physical access roster for the [redacted] production environment server room. On October 21, 2024, Assistant Commandant for Resources officials provided a physical access roster to demonstrate the completion of the corrective actions.

### *(U) Our Response*

~~(CUI)~~ Comments from the Deputy Assistant Commandant addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. Although Assistant Commandant for Resources officials provided a physical access roster, the roster did not identify whether it applied to the [redacted] production environment server room, and therefore, the roster was not adequate to close the recommendation. We will close the recommendation once the [redacted] provides an updated physical access roster that indicates it applies to the [redacted] production environment server room.

b. **~~(CUI)~~ Develop and implement procedures to update, when appropriate, the physical access roster for the [redacted] production environment server room at [redacted].**

### *~~(CUI)~~ [redacted] Comments*

~~(CUI)~~ The Deputy Assistant Commandant for Resources, responding for the [redacted], agreed, stating that the [redacted] developed and implemented procedures to update the physical access roster for the [redacted] production environment server room. On October 21, 2024, Assistant Commandant for Resources officials provided a [redacted] access request form to demonstrate the completion of the corrective actions.

## (U) Our Response

~~(CUI)~~ Comments from the Deputy Assistant Commandant addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. Although Assistant Commandant for Resources officials provided an access request form, the form did not include procedures describing how to update the physical access roster for the [redacted] production environment server room, and therefore, we could not close the recommendation based on the form. We will close the recommendation once the [redacted] provides the procedures.

c. **~~(CUI)~~ Develop and implement physical security methods to control and monitor physical access to the [redacted] [redacted] production environment server room at [redacted] [redacted], in accordance with Department of Defense physical security requirements for information technology.**

## ~~(CUI)~~ [redacted] Comments

~~(CUI)~~ The Deputy Assistant Commandant for Resources, responding for the [redacted], agreed, stating that the [redacted] developed and implemented physical security methods to control and monitor physical access to the [redacted] production environment server room. On October 21, 2024, Assistant Commandant for Resources officials provided documents to demonstrate the completion of the corrective actions.

## (U) Our Response

~~(CUI)~~ Comments from the Deputy Assistant Commandant partially addressed the recommendation; therefore, the recommendation is unresolved. Although the Deputy Assistant Commandant stated that the [redacted] [redacted] implemented methods to control and monitor physical access to the server room, we could not determine the specific methods implemented based on a review of the documents provided. Therefore, we request that the [redacted] [redacted] provide additional comments, within 30 days of the final report, to specify the physical security methods developed and implemented to control and monitor physical access to the [redacted] production environment server room.

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

### *~~(CUI)~~* [redacted]

~~(CUI)~~ The Deputy Assistant Commandant for Resources, responding for the [redacted], agreed, stating that the [redacted]. The Deputy Assistant Commandant expected that the [redacted] would complete these actions by December 31, 2024.

### *(U) Our Response*

~~(CUI)~~ Comments from the Deputy Assistant Commandant addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the [redacted].

## *(U) Recommendation 4*

**(U) We recommend that the Commander, Coast Guard Cyber Command:**

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

### *(U) Coast Guard Cyber Command Comments*

~~(CUI)~~ The Deputy Assistant Commandant for Resources, responding for the CGCYBER Commander, agreed, stating that the Commander would [redacted]. The Deputy Assistant Commandant expected that the CGCYBER Commander would complete these actions by June 30, 2025.

### *(U) Our Response*

~~(CUI)~~ Comments from the Deputy Assistant Commandant addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CGCYBER Commander provides a copy of the [redacted].

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

## (U) Coast Guard Cyber Command Comments

~~(CUI)~~ The Deputy Assistant Commandant for Resources, responding for the CGCYBER Commander, agreed, stating that the Commander would [redacted]. The Deputy Assistant Commandant also stated that the [redacted]. The Deputy Assistant Commandant expected that the CGCYBER Commander would complete these actions by September 30, 2025.

## (U) Our Response

~~(CUI)~~ Comments from the Deputy Assistant Commandant addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CGCYBER Commander provides documents that demonstrate the [redacted].

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

## (U) Coast Guard Cyber Command Comments

~~(CUI)~~ The Deputy Assistant Commandant for Resources, responding for the CGCYBER Commander, agreed, stating that the Commander and Coast Guard CIO would [redacted]. The Deputy Assistant Commandant expected that the CGCYBER Commander and Coast Guard CIO would complete these actions by September 30, 2025.

## (U) Our Response

~~(CUI)~~ Comments from the Deputy Assistant Commandant addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CGCYBER Commander provides documents that demonstrate the CGCYBER Commander [redacted].

d. **(U) Direct the security control assessors to conduct and document the results of annual security assessments in accordance with established control assessment frequencies for Coast Guard information systems and ensure that the security control assessors are independent of the system that they assess.**

## (U) Coast Guard Cyber Command Comments

~~(CUI)~~ The Deputy Assistant Commandant for Resources, responding for the CGCYBER Commander, agreed but did not identify any actions to implement the recommendation. Instead, the Deputy Assistant Commandant stated that the SCAs followed DoD policy for assessing security controls in accordance with the frequencies identified in the enterprise Mission Assurance Support Service (eMASS) system, which range from [redacted].[53] The Deputy Assistant Commandant added that the SCAs were independent of the systems they assessed because they were assigned under a different command structure than the commands that built, configured, and deployed systems.

## (U) Our Response

~~(CUI)~~ Comments from the Deputy Assistant Commandant did not address the specifics of the recommendation; therefore, the recommendation is unresolved. Although the Deputy Assistant Commandant stated that the SCAs followed DoD policy and conducted assessments from [redacted], DoD policy does not establish assessment frequencies for security controls. Instead, the DoD CIO requires each DoD Component to establish its own frequencies for each security control. Therefore, if the Coast Guard security control assessment frequencies range from [redacted], then the CGCYBER SCAs should assess every control for a Coast Guard system [redacted]. However, as identified in this report, the CGCYBER SCAs assessed only 20.4 percent,

[53] (U) The eMASS system is a web-based cybersecurity governance, risk, and compliance tool that allows information system owners, testers, and SCAs to collaborate effectively and execute security assessments on Coast Guard information systems.

~~(CUI)~~ 37.5 percent, and 1.5 percent of all cybersecurity controls for the [redacted] [redacted] systems, respectively, during FY 2022 and FY 2023. Furthermore, the Coast Guard SCAs had not prepared security assessment reports to document their results for the [redacted] systems since 2018, even though this is a DoD requirement. Therefore, we revised the finding and recommendation to clarify that SCAs are responsible for conducting and documenting the results of annual security assessments in accordance with established control assessment frequencies for Coast Guard systems.

(U) Although we agree that the CGCYBER SCAs were not officially assigned to the system owners responsible for building, configuring, and deploying Coast Guard systems, the SCAs were unofficially performing ISSM duties for the systems, which created conflicts of interest because ISSMs work on behalf of system owners. The Coast Guard SISO may resolve the conflicts of interest by identifying an ISSM for each Coast Guard system in response to Recommendation 1.e, as long as the SCAs are otherwise independent of the system owners.

(U) Therefore, we request that the CGCYBER Commander provide additional comments, within 30 days of the final report, to specify how they plan to direct the SCAs to conduct and document the results of annual security control assessments and how they will ensure that the SCAs are independent of systems that they assess.

e. **~~(CUI)~~ Issue authorization decisions for all Coast Guard systems operating under Coast Guard Ongoing Authorization, including the [redacted] [redacted] systems.**

## *(U) Coast Guard Cyber Command Comments*

(U) The Deputy Assistant Commandant for Resources, responding for the CGCYBER Commander, agreed, stating that the CGCYBER Commander issued authorization decisions for all Coast Guard systems under the Ongoing Authorization Program. The Deputy Assistant Commandant stated that the CGCYBER Commander completed these actions as of September 30, 2024.

## *(U) Our Response*

(U) Comments from the Deputy Assistant Commandant addressed all specifics of the recommendation. We verified that the CGCYBER Commander issued the authorization decisions for all Coast Guard systems that were operating under Coast Guard Ongoing Authorization. Therefore, this recommendation is closed.

## (U) Recommendation 5

**(U) We recommend that the Department of Defense Chief Information Officer develop and implement a process to ensure that the Coast Guard complies with Department of Defense requirements for obtaining authorizations to operate for information systems operating on the Department of Defense Information Network.**

### (U) DoD Chief Information Officer Comments

(U) The Acting DoD CIO disagreed, stating that the DoD already has a well-established and effective process to ensure the Coast Guard complies with DoD requirements for obtaining ATOs. The Acting DoD CIO stated that they would continue to monitor the Coast Guard's compliance with DoD requirements for obtaining ATOs through the Cybersecurity Hardening Scorecard and the eMASS system.

### (U) Our Response

(U) Comments from the Acting DoD CIO did not address the specifics of the recommendation; therefore, the recommendation is unresolved. Although the Acting DoD CIO stated that the DoD has a well-established and effective process to ensure all systems comply with ATO requirements, we identified during the audit that the Coast Guard was operating 38 systems on the DODIN without ATOs and in violation of DoD requirements. If the DoD's process was effective, the DoD should have detected that these 38 Coast Guard systems were operating without ATOs and directed the Coast Guard to take corrective actions as early as August 2021. Therefore, we request that the Acting DoD CIO, within 30 days of the final report, provide additional comments to specify how they will develop and implement a process that is sufficient to ensure that the Coast Guard complies with the requirements for obtaining ATOs for information systems operating on the DODIN.

# (U) Appendix

## (U) Scope and Methodology

(U) We conducted this performance audit from May 2021 through September 2024 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) Due to the magnitude of audit staff turnover since we announced the audit in May 2021, we conducted additional site visits and testing from April 2023 through August 2023. The results of those site visits and testing form the basis of the findings and recommendations of this report and therefore are relevant to the Coast Guard's existing operations.

~~(CUI)~~ We identified [redacted] unclassified Coast Guard information systems operating on the DODIN as of June 2021 and obtained information on the overall risks for these systems from the eMASS system. From the [redacted] systems, we selected the [redacted] [redacted] systems for review. An information system's potential impact is the degree of harm (low, medium, or high) that an information owner believes may result from the loss of confidentiality, integrity, and availability if a security breach occurs. In addition, we selected to review cybersecurity controls from seven NIST Special Publication 800-53, Revision 4 control families: access control, security assessment and authorization, contingency planning, [redacted], physical and environmental protection, personnel security, and risk assessment.[54]

~~(CUI)~~ We reviewed NIST, DoD, DHS, and Coast Guard policies and guidance to identify specific cybersecurity requirements applicable to the Coast Guard systems operating on the DODIN. In addition, we obtained and analyzed documentation related to security controls selected for audit, including vulnerability scans, contingency planning documentation, physical access rosters and related credentials, and documents that are part of the security authorization packages for the [redacted] systems.

[54] (U) For this audit, we reviewed NIST Special Publication 800-53, Revision 4. Although NIST Special Publication 800-53 was issued up to Revision 5, at the time of the audit, the DoD and DHS required organizations to follow Revision 4.

~~(CUI)~~ We met with Coast Guard officials responsible for the selection, assessment, and approval of system security controls for the [redacted] systems. In addition, we met with Coast Guard officials responsible for implementing physical and environmental controls for the [redacted] systems.

~~(CUI)~~ We conducted site visits and reviewed Coast Guard server rooms located at the [redacted], to determine whether Coast Guard officials implemented cybersecurity controls to protect servers that were critical to the [redacted] systems.

(U) This report was reviewed by DoD and DHS officials associated with this project to identify whether any of their reported information, including legacy FOUO information, should be safeguarded and marked in accordance with the DoD CUI Program. We considered comments submitted by those officials when marking this report. If the DoD and DHS officials failed to provide any or sufficient comments about the markings, we marked the report based on our assessment of the information.

## (U) Internal Control Assessment and Compliance

~~(CUI)~~ We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. Specifically, we reviewed and assessed internal controls related to the implementation of cybersecurity requirements for Coast Guard information systems on the DODIN. Our review included policies and procedures in place, oversight, and accountability for the implementation of security controls for the [redacted] systems. However, because our review was limited to these internal control components and underlying principles, it may not disclose all internal control deficiencies that may have existed during the time of the audit.

## (U) Use of Computer-Processed Data

(U) We used computer-processed data from the eMASS system to identify the total number of available Coast Guard systems for review. We determined that the total number of Coast Guard systems and their overall risks was sufficient and reliable for the purpose of identifying systems to review.

## (U) Use of Technical Assistance

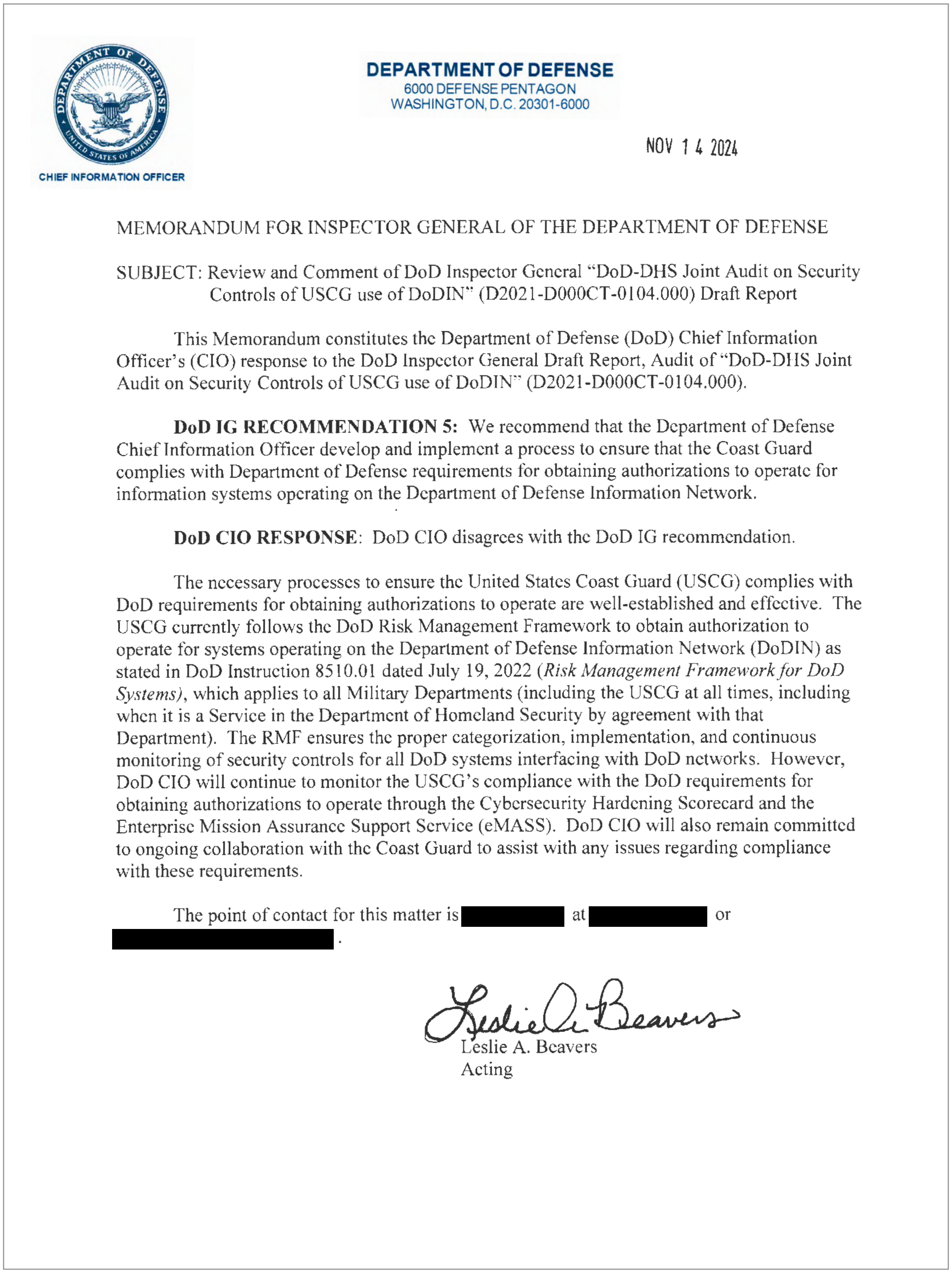
(U) We relied upon technical assistance for this audit. DoD OIG information technology specialists advised us on the selection of information technology systems and networks to review during the audit. DoD OIG information technology specialists also analyzed documentation related to technical processes to aid the team in determining if security control implementation was sufficient according to applicable DoD requirements.

## (U) Prior Coverage

(U) No prior coverage has been conducted on the Coast Guard's implementation of cybersecurity controls for systems operating on the DODIN during the last 5 years.

# (U) Management Comments

## (U) Acting Department of Defense Chief Information Officer



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

NOV 14 2024

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment of DoD Inspector General "DoD-DHS Joint Audit on Security Controls of USCG use of DoDIN" (D2021-D000CT-0104.000) Draft Report

This Memorandum constitutes the Department of Defense (DoD) Chief Information Officer's (CIO) response to the DoD Inspector General Draft Report, Audit of "DoD-DHS Joint Audit on Security Controls of USCG use of DoDIN" (D2021-D000CT-0104.000).

**DoD IG RECOMMENDATION 5:** We recommend that the Department of Defense Chief Information Officer develop and implement a process to ensure that the Coast Guard complies with Department of Defense requirements for obtaining authorizations to operate for information systems operating on the Department of Defense Information Network.

**DoD CIO RESPONSE**: DoD CIO disagrees with the DoD IG recommendation.

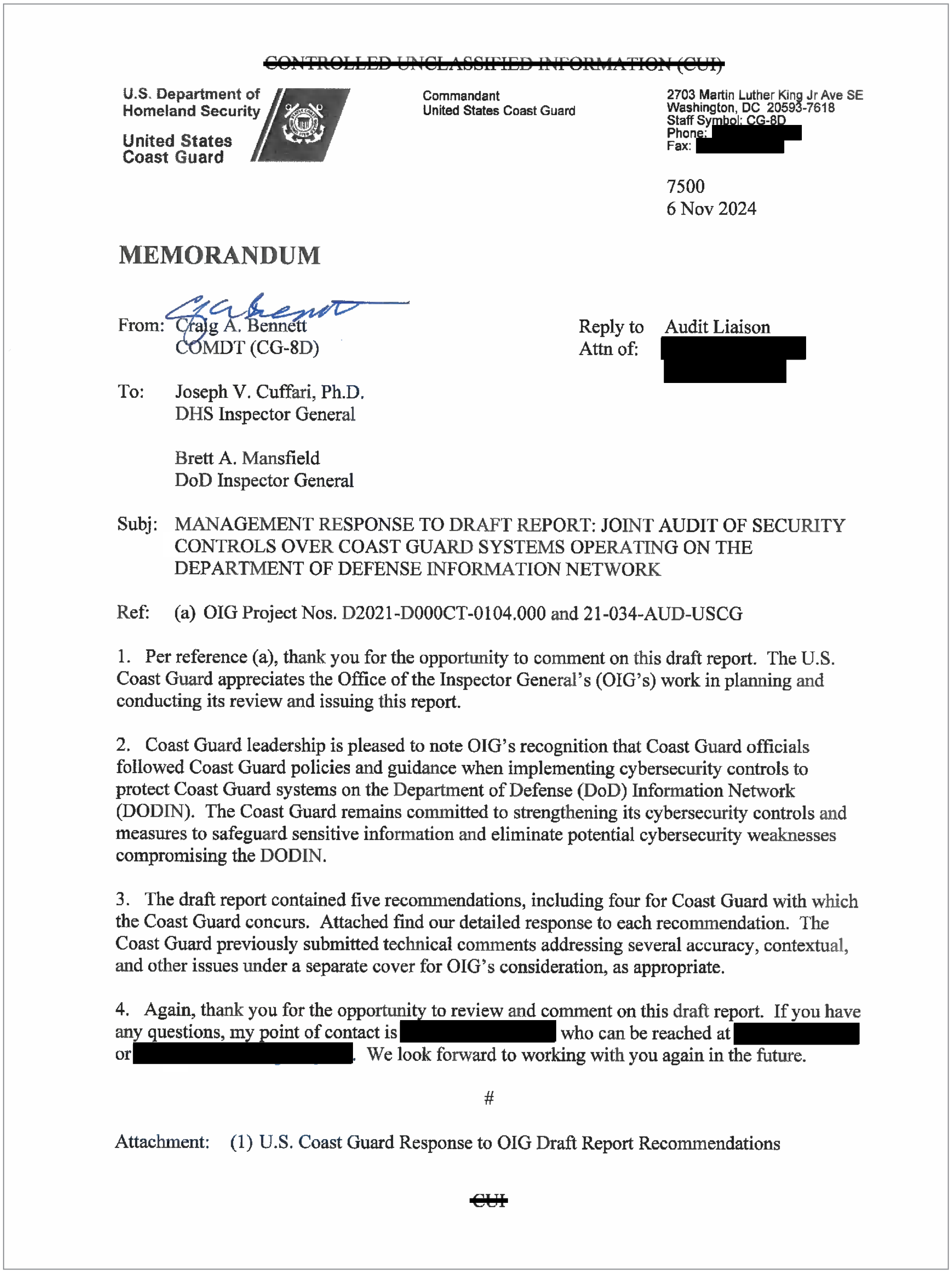
The necessary processes to ensure the United States Coast Guard (USCG) complies with DoD requirements for obtaining authorizations to operate are well-established and effective. The USCG currently follows the DoD Risk Management Framework to obtain authorization to operate for systems operating on the Department of Defense Information Network (DoDIN) as stated in DoD Instruction 8510.01 dated July 19, 2022 (*Risk Management Framework for DoD Systems)*, which applies to all Military Departments (including the USCG at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department). The RMF ensures the proper categorization, implementation, and continuous monitoring of security controls for all DoD systems interfacing with DoD networks. However, DoD CIO will continue to monitor the USCG's compliance with the DoD requirements for obtaining authorizations to operate through the Cybersecurity Hardening Scorecard and the Enterprise Mission Assurance Support Service (eMASS). DoD CIO will also remain committed to ongoing collaboration with the Coast Guard to assist with any issues regarding compliance with these requirements.

The point of contact for this matter is [redacted] at [redacted] or [redacted].

Leslie A. Beavers

Leslie A. Beavers
Acting

## (U) Deputy Assistant Commandant for Resources



~~CONTROLLED UNCLASSIFIED INFORMATION (CUI)~~

U.S. Department of
Homeland Security

United States
Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Jr Ave SE
Washington, DC 20593-7618
Staff Symbol: CG-8D
Phone: [redacted]
Fax: [redacted]

7500
6 Nov 2024

**MEMORANDUM**

From: Craig A. Bennett
COMDT (CG-8D)

Reply to Audit Liaison
Attn of: [redacted]

To: Joseph V. Cuffari, Ph.D.
DHS Inspector General

Brett A. Mansfield
DoD Inspector General

Subj: MANAGEMENT RESPONSE TO DRAFT REPORT: JOINT AUDIT OF SECURITY CONTROLS OVER COAST GUARD SYSTEMS OPERATING ON THE DEPARTMENT OF DEFENSE INFORMATION NETWORK

Ref: (a) OIG Project Nos. D2021-D000CT-0104.000 and 21-034-AUD-USCG

1. Per reference (a), thank you for the opportunity to comment on this draft report. The U.S. Coast Guard appreciates the Office of the Inspector General's (OIG's) work in planning and conducting its review and issuing this report.

2. Coast Guard leadership is pleased to note OIG's recognition that Coast Guard officials followed Coast Guard policies and guidance when implementing cybersecurity controls to protect Coast Guard systems on the Department of Defense (DoD) Information Network (DODIN). The Coast Guard remains committed to strengthening its cybersecurity controls and measures to safeguard sensitive information and eliminate potential cybersecurity weaknesses compromising the DODIN.

3. The draft report contained five recommendations, including four for Coast Guard with which the Coast Guard concurs. Attached find our detailed response to each recommendation. The Coast Guard previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for OIG's consideration, as appropriate.

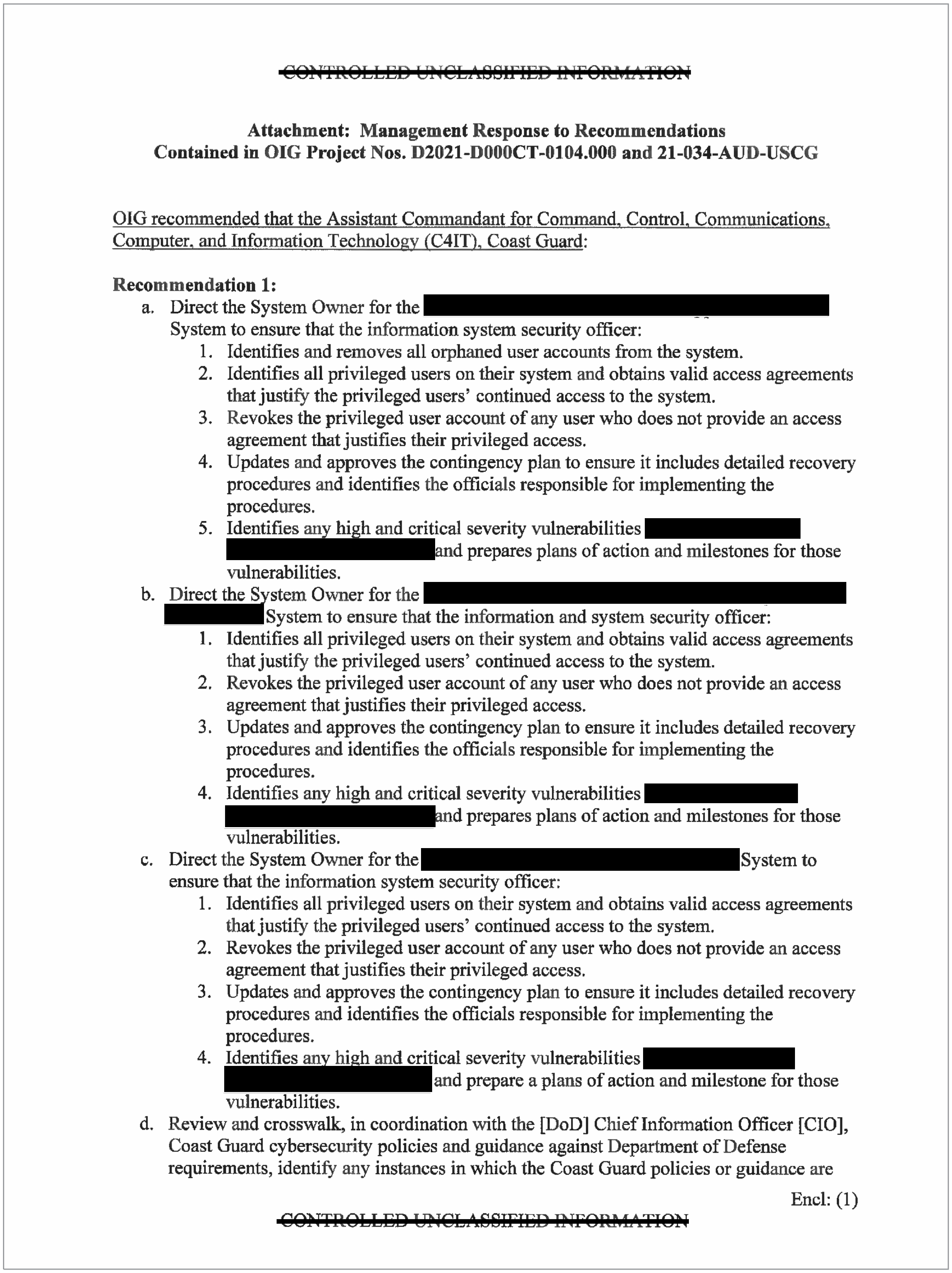
4. Again, thank you for the opportunity to review and comment on this draft report. If you have any questions, my point of contact is [redacted] who can be reached at [redacted] or [redacted]. We look forward to working with you again in the future.

#

Attachment: (1) U.S. Coast Guard Response to OIG Draft Report Recommendations

~~CUI~~

# (U) Deputy Assistant Commandant for Resources (cont'd)



~~CONTROLLED UNCLASSIFIED INFORMATION~~

**Attachment: Management Response to Recommendations**
**Contained in OIG Project Nos. D2021-D000CT-0104.000 and 21-034-AUD-USCG**

<u>OIG recommended that the Assistant Commandant for Command, Control, Communications, Computer, and Information Technology (C4IT), Coast Guard</u>:

**Recommendation 1:**

a. Direct the System Owner for the [redacted] System to ensure that the information system security officer:
   1. Identifies and removes all orphaned user accounts from the system.
   2. Identifies all privileged users on their system and obtains valid access agreements that justify the privileged users' continued access to the system.
   3. Revokes the privileged user account of any user who does not provide an access agreement that justifies their privileged access.
   4. Updates and approves the contingency plan to ensure it includes detailed recovery procedures and identifies the officials responsible for implementing the procedures.
   5. Identifies any high and critical severity vulnerabilities [redacted] and prepares plans of action and milestones for those vulnerabilities.

b. Direct the System Owner for the [redacted] System to ensure that the information and system security officer:
   1. Identifies all privileged users on their system and obtains valid access agreements that justify the privileged users' continued access to the system.
   2. Revokes the privileged user account of any user who does not provide an access agreement that justifies their privileged access.
   3. Updates and approves the contingency plan to ensure it includes detailed recovery procedures and identifies the officials responsible for implementing the procedures.
   4. Identifies any high and critical severity vulnerabilities [redacted] and prepares plans of action and milestones for those vulnerabilities.

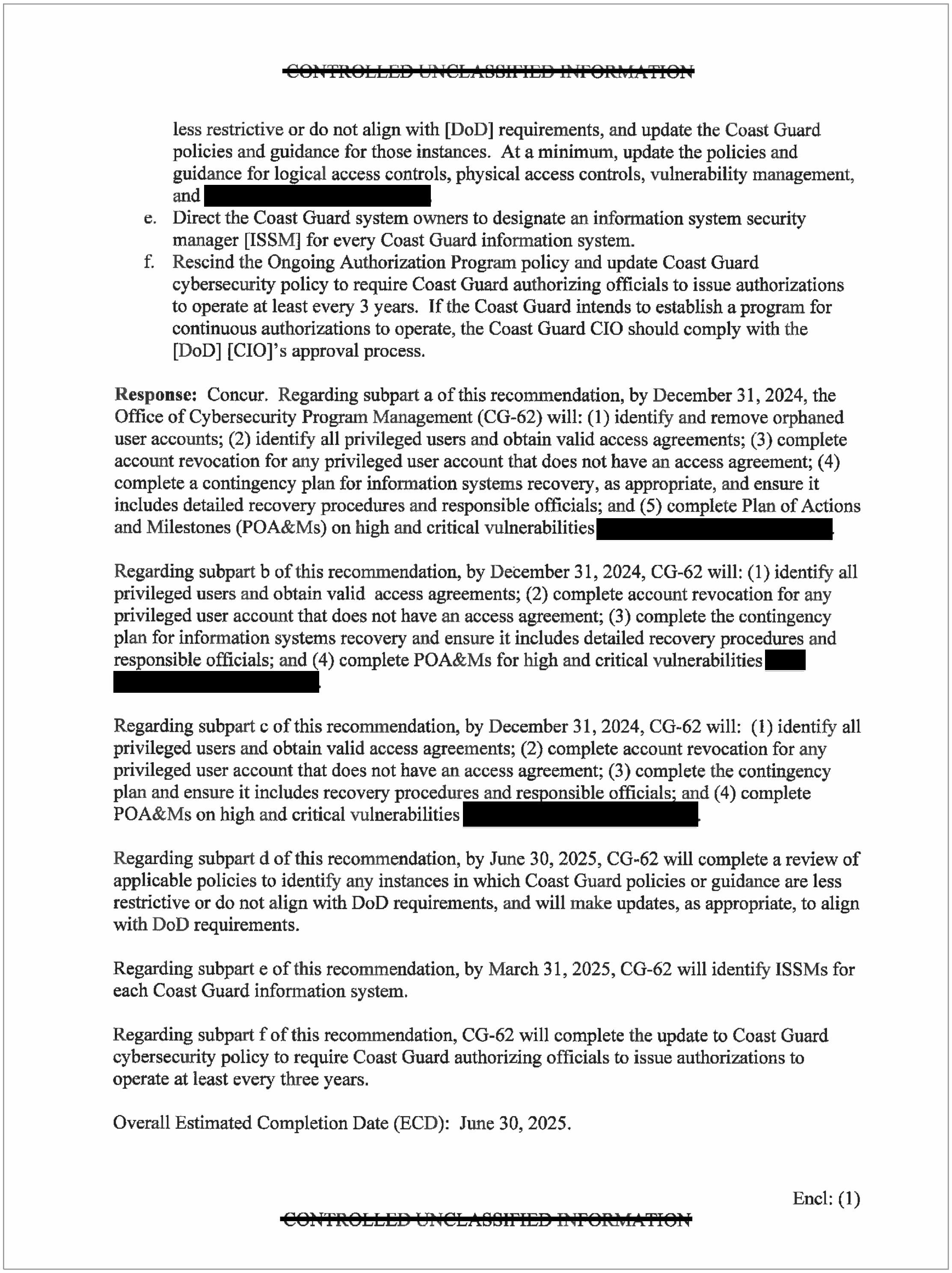
c. Direct the System Owner for the [redacted] System to ensure that the information system security officer:
   1. Identifies all privileged users on their system and obtains valid access agreements that justify the privileged users' continued access to the system.
   2. Revokes the privileged user account of any user who does not provide an access agreement that justifies their privileged access.
   3. Updates and approves the contingency plan to ensure it includes detailed recovery procedures and identifies the officials responsible for implementing the procedures.
   4. Identifies any high and critical severity vulnerabilities [redacted] and prepare a plans of action and milestone for those vulnerabilities.

d. Review and crosswalk, in coordination with the [DoD] Chief Information Officer [CIO], Coast Guard cybersecurity policies and guidance against Department of Defense requirements, identify any instances in which the Coast Guard policies or guidance are

Encl: (1)

~~CONTROLLED UNCLASSIFIED INFORMATION~~

## (U) Deputy Assistant Commandant for Resources (cont'd)



~~CONTROLLED UNCLASSIFIED INFORMATION~~

less restrictive or do not align with [DoD] requirements, and update the Coast Guard policies and guidance for those instances. At a minimum, update the policies and guidance for logical access controls, physical access controls, vulnerability management, and [redacted].

e. Direct the Coast Guard system owners to designate an information system security manager [ISSM] for every Coast Guard information system.

f. Rescind the Ongoing Authorization Program policy and update Coast Guard cybersecurity policy to require Coast Guard authorizing officials to issue authorizations to operate at least every 3 years. If the Coast Guard intends to establish a program for continuous authorizations to operate, the Coast Guard CIO should comply with the [DoD] [CIO]'s approval process.

**Response:** Concur. Regarding subpart a of this recommendation, by December 31, 2024, the Office of Cybersecurity Program Management (CG-62) will: (1) identify and remove orphaned user accounts; (2) identify all privileged users and obtain valid access agreements; (3) complete account revocation for any privileged user account that does not have an access agreement; (4) complete a contingency plan for information systems recovery, as appropriate, and ensure it includes detailed recovery procedures and responsible officials; and (5) complete Plan of Actions and Milestones (POA&Ms) on high and critical vulnerabilities [redacted].

Regarding subpart b of this recommendation, by December 31, 2024, CG-62 will: (1) identify all privileged users and obtain valid access agreements; (2) complete account revocation for any privileged user account that does not have an access agreement; (3) complete the contingency plan for information systems recovery and ensure it includes detailed recovery procedures and responsible officials; and (4) complete POA&Ms for high and critical vulnerabilities [redacted].

Regarding subpart c of this recommendation, by December 31, 2024, CG-62 will: (1) identify all privileged users and obtain valid access agreements; (2) complete account revocation for any privileged user account that does not have an access agreement; (3) complete the contingency plan and ensure it includes recovery procedures and responsible officials; and (4) complete POA&Ms on high and critical vulnerabilities [redacted].

Regarding subpart d of this recommendation, by June 30, 2025, CG-62 will complete a review of applicable policies to identify any instances in which Coast Guard policies or guidance are less restrictive or do not align with DoD requirements, and will make updates, as appropriate, to align with DoD requirements.

Regarding subpart e of this recommendation, by March 31, 2025, CG-62 will identify ISSMs for each Coast Guard information system.

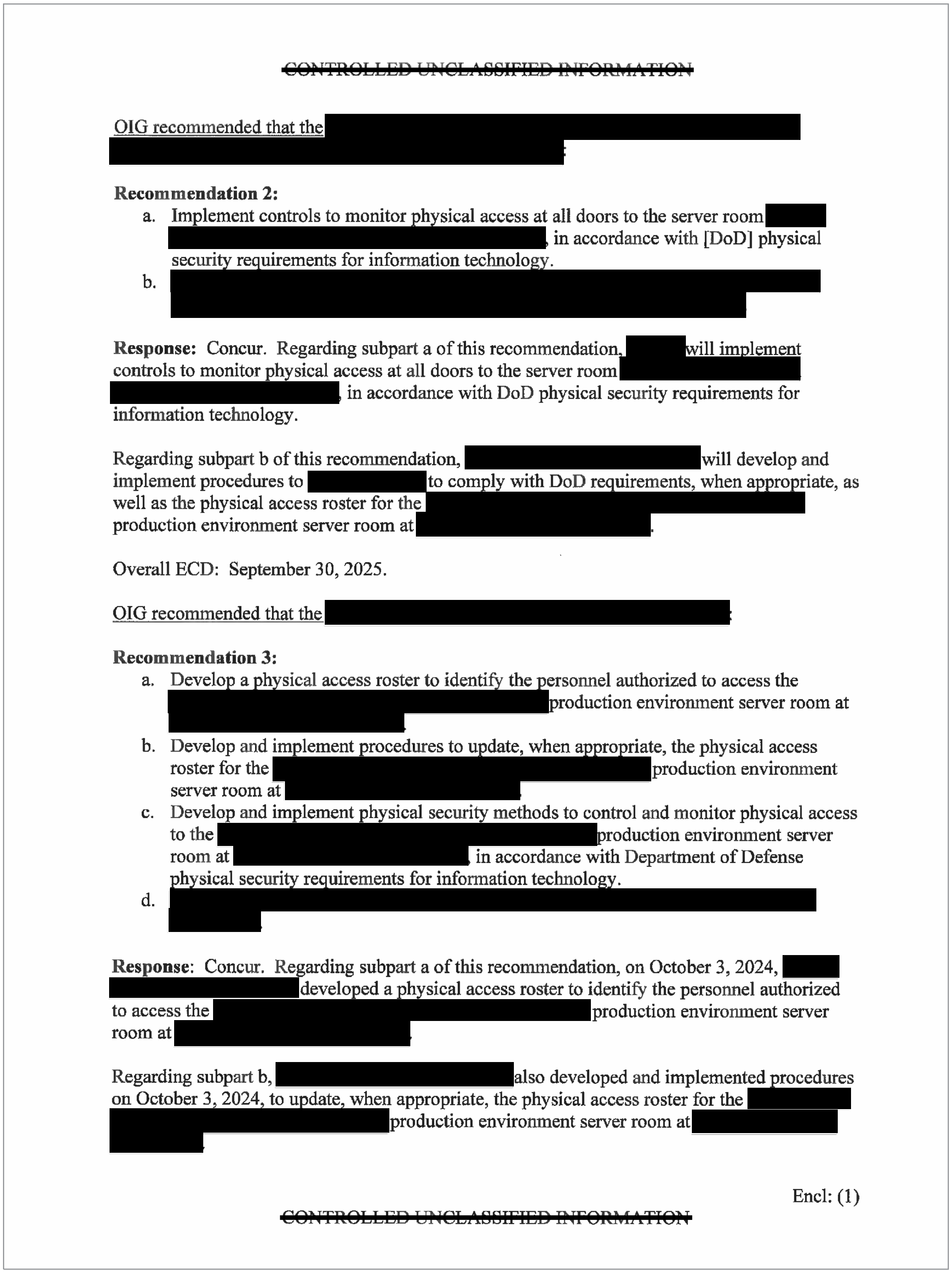
Regarding subpart f of this recommendation, CG-62 will complete the update to Coast Guard cybersecurity policy to require Coast Guard authorizing officials to issue authorizations to operate at least every three years.

Overall Estimated Completion Date (ECD): June 30, 2025.

Encl: (1)

~~CONTROLLED UNCLASSIFIED INFORMATION~~

## (U) Deputy Assistant Commandant for Resources (cont'd)



~~CONTROLLED UNCLASSIFIED INFORMATION~~

OIG recommended that the [redacted]:

**Recommendation 2:**

a. Implement controls to monitor physical access at all doors to the server room [redacted], in accordance with [DoD] physical security requirements for information technology.

b. [redacted]

**Response:** Concur. Regarding subpart a of this recommendation, [redacted] will implement controls to monitor physical access at all doors to the server room [redacted], in accordance with DoD physical security requirements for information technology.

Regarding subpart b of this recommendation, [redacted] will develop and implement procedures to [redacted] to comply with DoD requirements, when appropriate, as well as the physical access roster for the [redacted] production environment server room at [redacted].

Overall ECD: September 30, 2025.

OIG recommended that the [redacted]:

**Recommendation 3:**

a. Develop a physical access roster to identify the personnel authorized to access the [redacted] production environment server room at [redacted].

b. Develop and implement procedures to update, when appropriate, the physical access roster for the [redacted] production environment server room at [redacted].

c. Develop and implement physical security methods to control and monitor physical access to the [redacted] production environment server room at [redacted], in accordance with Department of Defense physical security requirements for information technology.

d. [redacted]

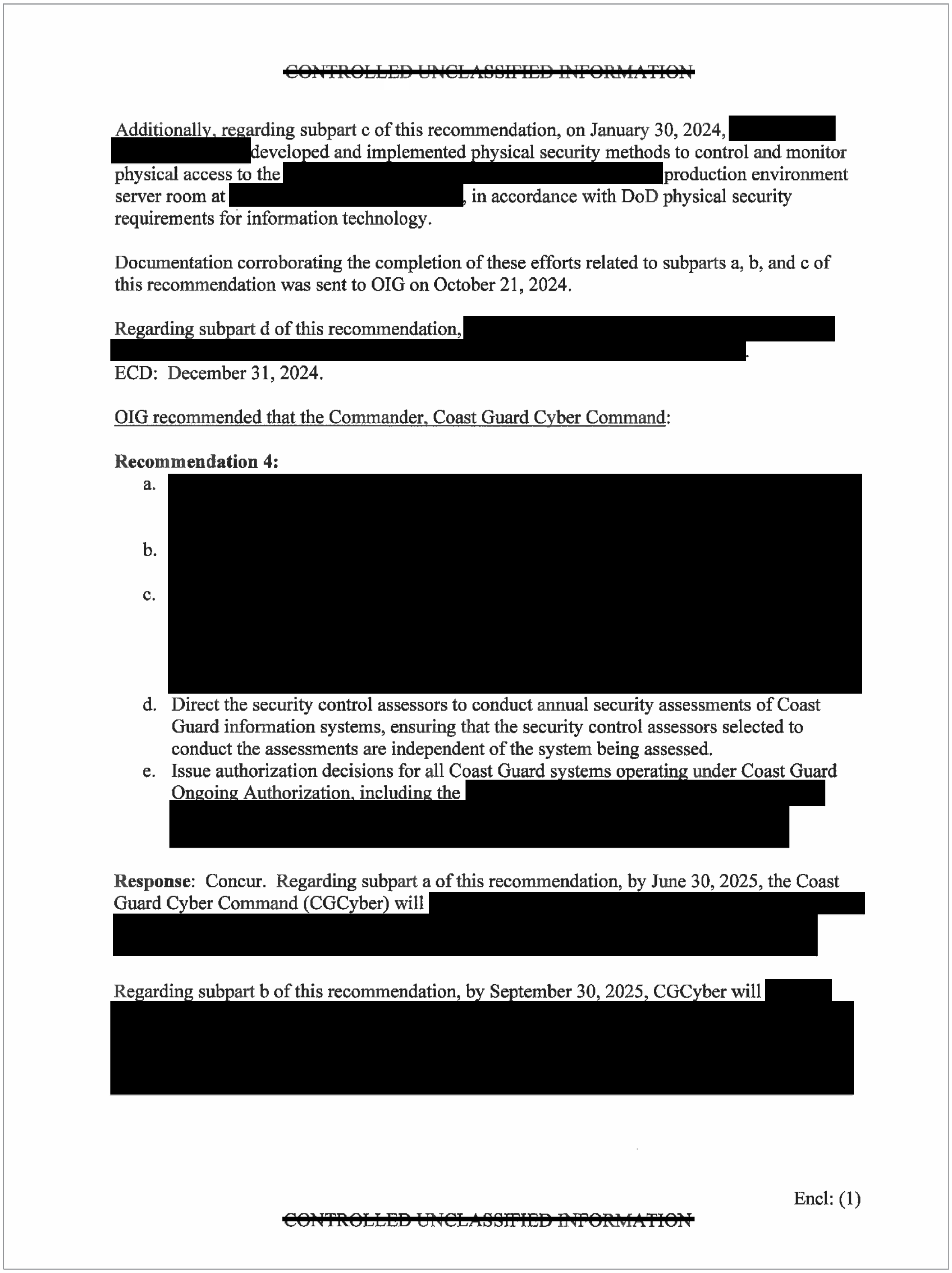
**Response:** Concur. Regarding subpart a of this recommendation, on October 3, 2024, [redacted] developed a physical access roster to identify the personnel authorized to access the [redacted] production environment server room at [redacted].

Regarding subpart b, [redacted] also developed and implemented procedures on October 3, 2024, to update, when appropriate, the physical access roster for the [redacted] production environment server room at [redacted]

Encl: (1)

~~CONTROLLED UNCLASSIFIED INFORMATION~~

## (U) Deputy Assistant Commandant for Resources (cont'd)



~~CONTROLLED UNCLASSIFIED INFORMATION~~

Additionally, regarding subpart c of this recommendation, on January 30, 2024, [redacted] developed and implemented physical security methods to control and monitor physical access to the [redacted] production environment server room at [redacted], in accordance with DoD physical security requirements for information technology.

Documentation corroborating the completion of these efforts related to subparts a, b, and c of this recommendation was sent to OIG on October 21, 2024.

Regarding subpart d of this recommendation, [redacted].

ECD: December 31, 2024.

OIG recommended that the Commander, Coast Guard Cyber Command:

**Recommendation 4:**

a. [redacted]

b.

c.

d. Direct the security control assessors to conduct annual security assessments of Coast Guard information systems, ensuring that the security control assessors selected to conduct the assessments are independent of the system being assessed.

e. Issue authorization decisions for all Coast Guard systems operating under Coast Guard Ongoing Authorization, including the [redacted]

**Response**: Concur. Regarding subpart a of this recommendation, by June 30, 2025, the Coast Guard Cyber Command (CGCyber) will [redacted]

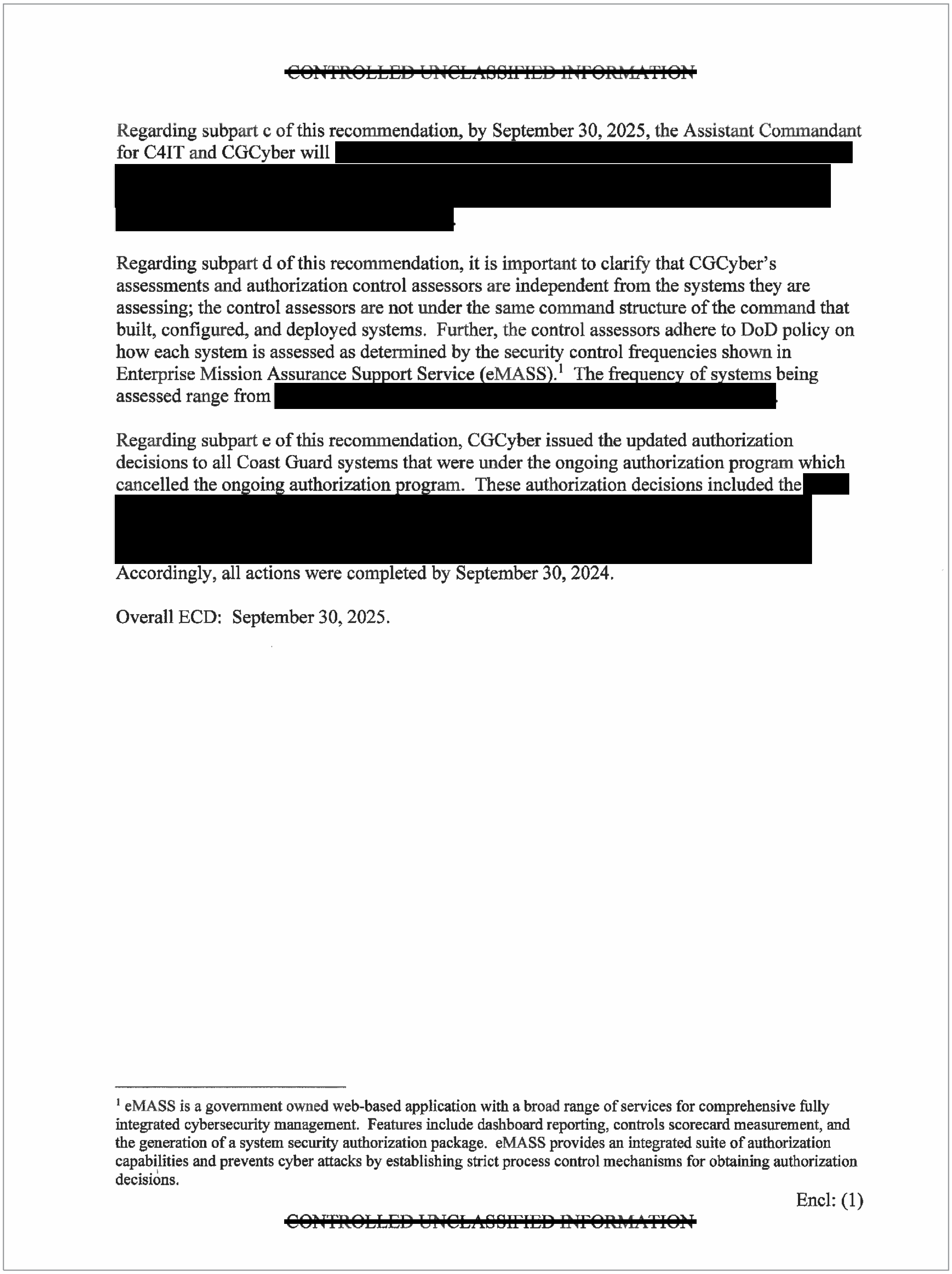
Regarding subpart b of this recommendation, by September 30, 2025, CGCyber will [redacted]

Encl: (1)

~~CONTROLLED UNCLASSIFIED INFORMATION~~

# (U) Deputy Assistant Commandant for Resources (cont'd)

**Final Report Reference**



~~CONTROLLED UNCLASSIFIED INFORMATION~~

Regarding subpart c of this recommendation, by September 30, 2025, the Assistant Commandant for C4IT and CGCyber will [redacted].

**Revised Page 22 and Recommendation 4.d**

Regarding subpart d of this recommendation, it is important to clarify that CGCyber's assessments and authorization control assessors are independent from the systems they are assessing; the control assessors are not under the same command structure of the command that built, configured, and deployed systems. Further, the control assessors adhere to DoD policy on how each system is assessed as determined by the security control frequencies shown in Enterprise Mission Assurance Support Service (eMASS).[1] The frequency of systems being assessed range from [redacted].

Regarding subpart e of this recommendation, CGCyber issued the updated authorization decisions to all Coast Guard systems that were under the ongoing authorization program which cancelled the ongoing authorization program. These authorization decisions included the [redacted] Accordingly, all actions were completed by September 30, 2024.

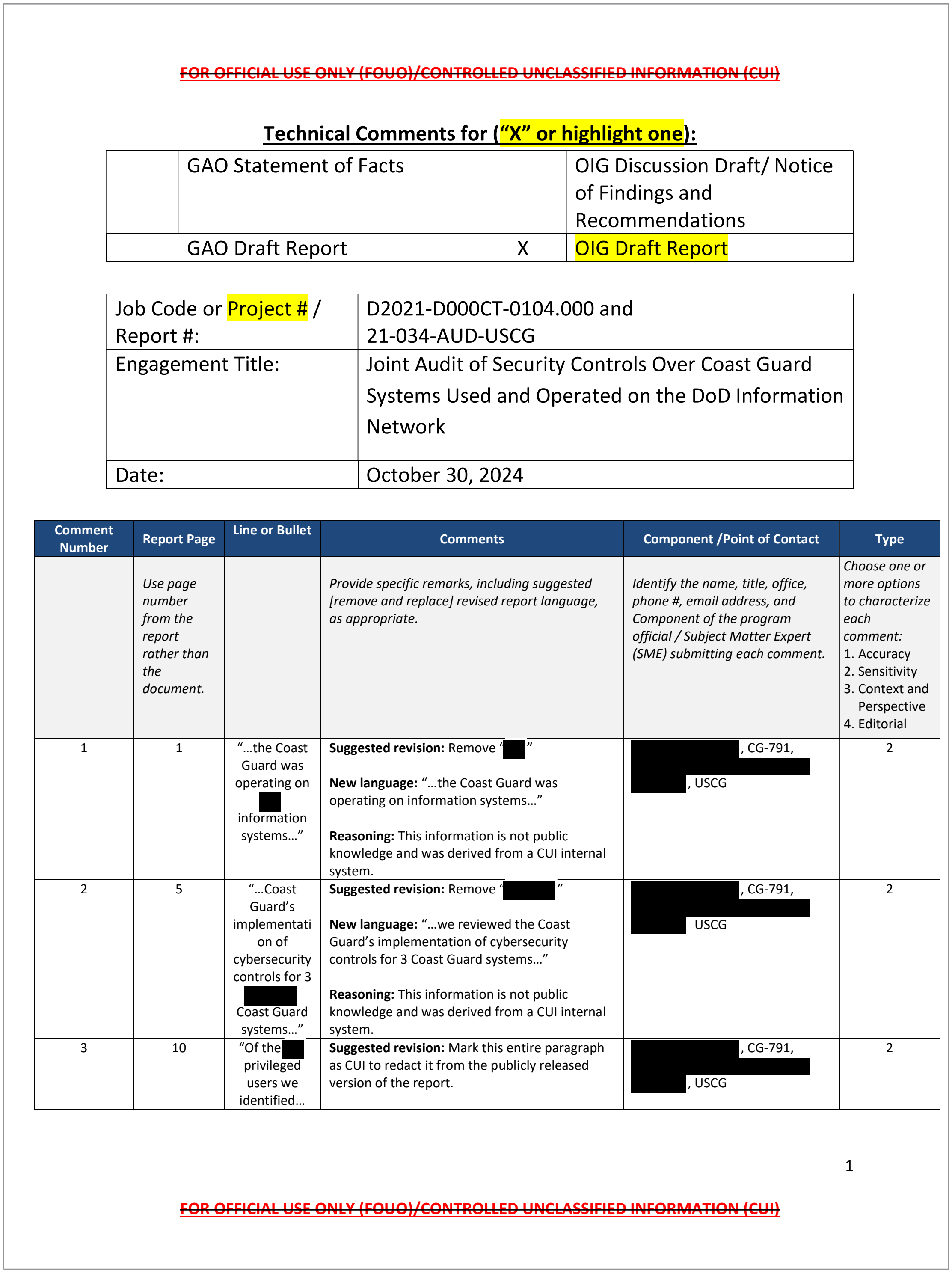
Overall ECD: September 30, 2025.

[1] eMASS is a government owned web-based application with a broad range of services for comprehensive fully integrated cybersecurity management. Features include dashboard reporting, controls scorecard measurement, and the generation of a system security authorization package. eMASS provides an integrated suite of authorization capabilities and prevents cyber attacks by establishing strict process control mechanisms for obtaining authorization decisions.

Encl: (1)

~~CONTROLLED UNCLASSIFIED INFORMATION~~

# (U) Deputy Assistant Commandant for Resources (cont'd)



~~FOR OFFICIAL USE ONLY (FOUO)/CONTROLLED UNCLASSIFIED INFORMATION (CUI)~~

**Technical Comments for ("X" or highlight one):**

| | | | |
|---|---|---|---|
| | GAO Statement of Facts | | OIG Discussion Draft/ Notice of Findings and Recommendations |
| | GAO Draft Report | X | OIG Draft Report |

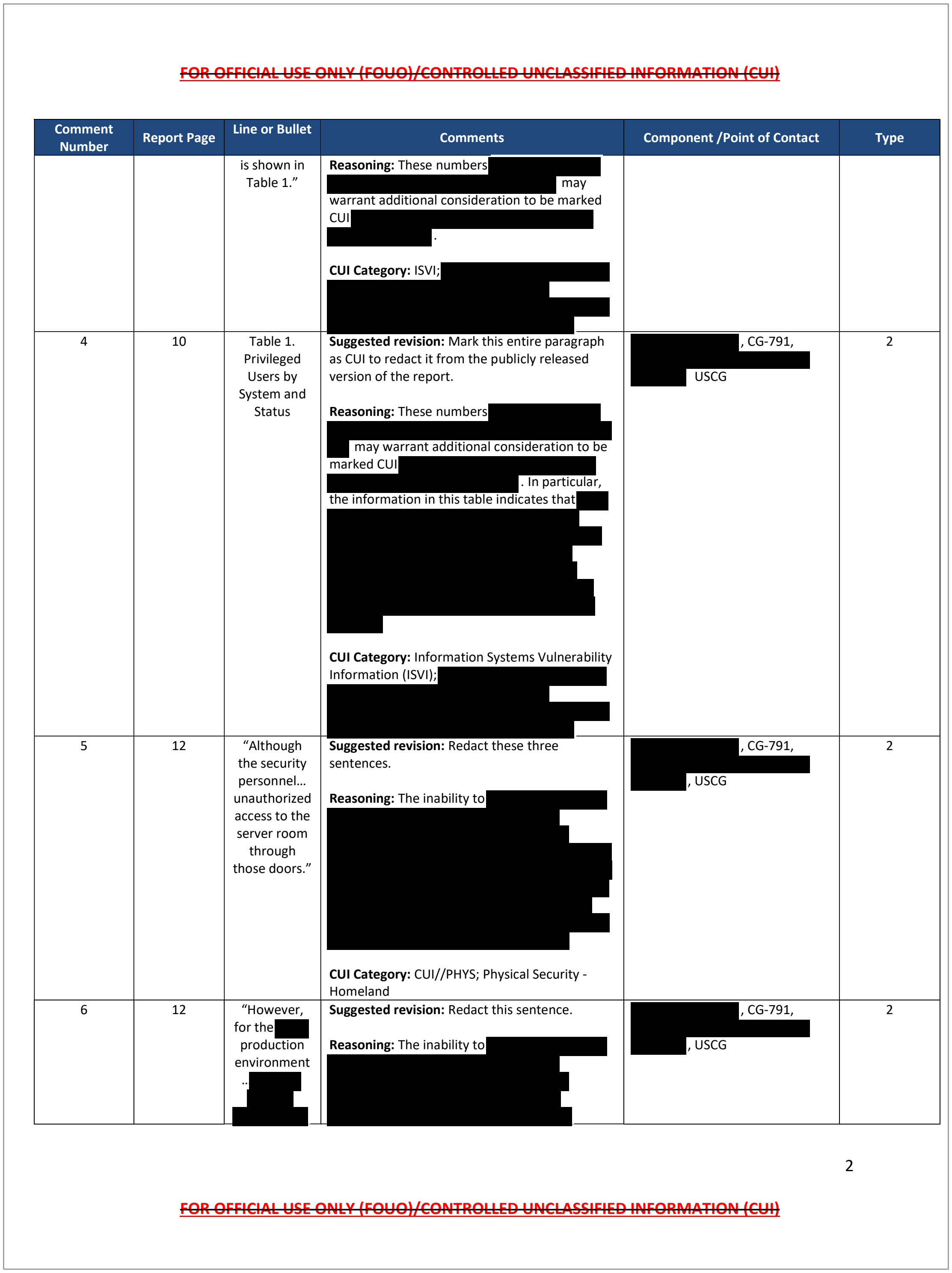
| | |
|---|---|
| Job Code or Project # / Report #: | D2021-D000CT-0104.000 and 21-034-AUD-USCG |
| Engagement Title: | Joint Audit of Security Controls Over Coast Guard Systems Used and Operated on the DoD Information Network |
| Date: | October 30, 2024 |

| Comment Number | Report Page | Line or Bullet | Comments | Component /Point of Contact | Type |
|---|---|---|---|---|---|
| | *Use page number from the report rather than the document.* | | *Provide specific remarks, including suggested [remove and replace] revised report language, as appropriate.* | *Identify the name, title, office, phone #, email address, and Component of the program official / Subject Matter Expert (SME) submitting each comment.* | *Choose one or more options to characterize each comment:*<br>1. Accuracy<br>2. Sensitivity<br>3. Context and Perspective<br>4. Editorial |
| 1 | 1 | "…the Coast Guard was operating on [redacted] information systems…" | **Suggested revision:** Remove '[redacted]'<br>**New language:** "…the Coast Guard was operating on information systems…"<br>**Reasoning:** This information is not public knowledge and was derived from a CUI internal system. | [redacted], CG-791, [redacted], USCG | 2 |
| 2 | 5 | "…Coast Guard's implementation of cybersecurity controls for 3 [redacted] Coast Guard systems…" | **Suggested revision:** Remove '[redacted]'<br>**New language:** "…we reviewed the Coast Guard's implementation of cybersecurity controls for 3 Coast Guard systems…"<br>**Reasoning:** This information is not public knowledge and was derived from a CUI internal system. | [redacted], CG-791, [redacted] USCG | 2 |
| 3 | 10 | "Of the [redacted] privileged users we identified… | **Suggested revision:** Mark this entire paragraph as CUI to redact it from the publicly released version of the report. | [redacted], CG-791, [redacted], USCG | 2 |

1

~~FOR OFFICIAL USE ONLY (FOUO)/CONTROLLED UNCLASSIFIED INFORMATION (CUI)~~

# (U) Deputy Assistant Commandant for Resources (cont’d)



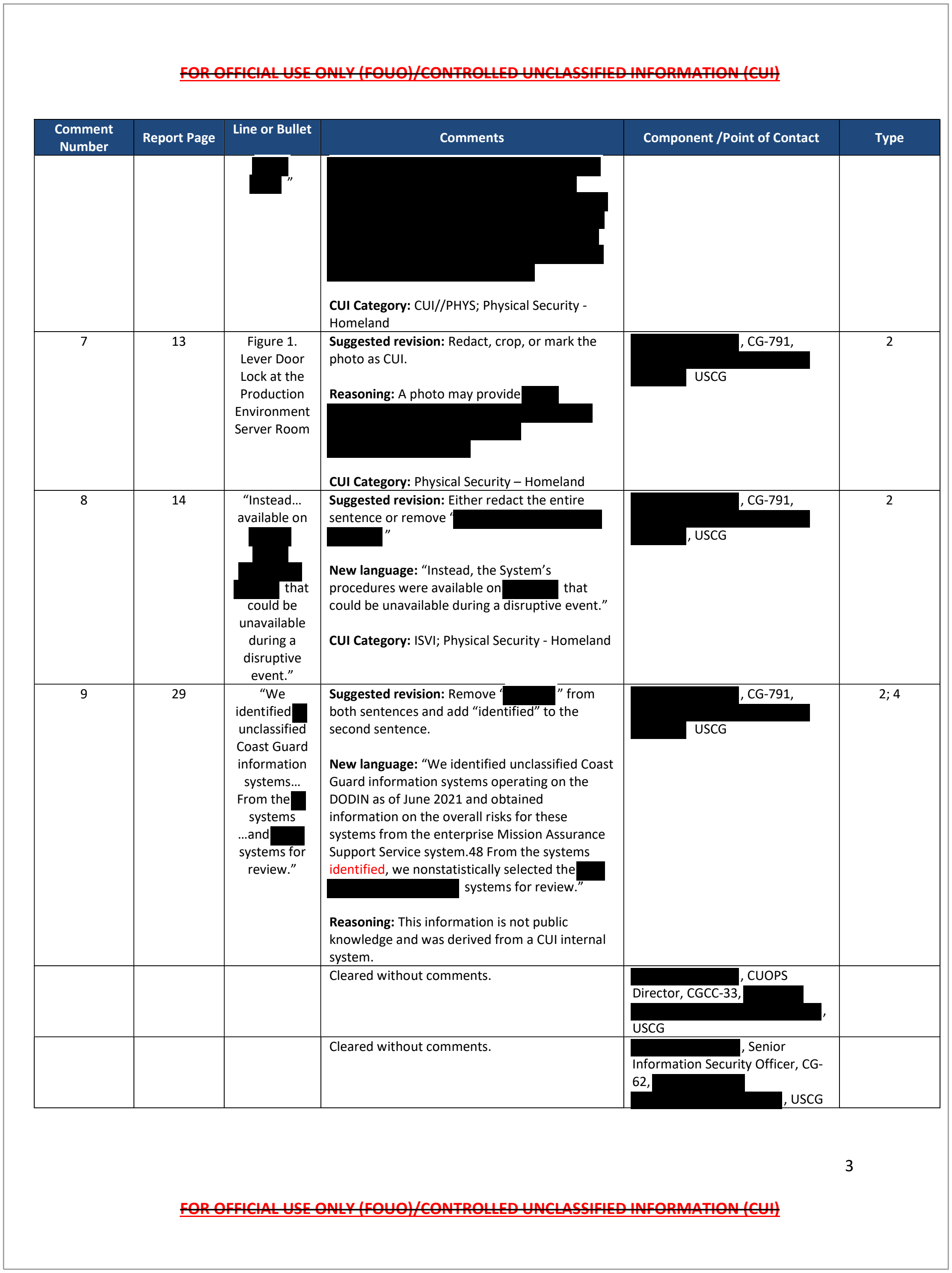
~~FOR OFFICIAL USE ONLY (FOUO)/CONTROLLED UNCLASSIFIED INFORMATION (CUI)~~

| Comment Number | Report Page | Line or Bullet | Comments | Component /Point of Contact | Type |
|---|---|---|---|---|---|
| | | is shown in Table 1.” | **Reasoning:** These numbers [redacted] may warrant additional consideration to be marked CUI [redacted].<br>**CUI Category:** ISVI; [redacted] | | |
| 4 | 10 | Table 1. Privileged Users by System and Status | **Suggested revision:** Mark this entire paragraph as CUI to redact it from the publicly released version of the report.<br>**Reasoning:** These numbers [redacted] may warrant additional consideration to be marked CUI [redacted]. In particular, the information in this table indicates that [redacted]<br>**CUI Category:** Information Systems Vulnerability Information (ISVI); [redacted] | [redacted], CG-791, [redacted] USCG | 2 |
| 5 | 12 | “Although the security personnel… unauthorized access to the server room through those doors.” | **Suggested revision:** Redact these three sentences.<br>**Reasoning:** The inability to [redacted]<br>**CUI Category:** CUI//PHYS; Physical Security - Homeland | [redacted], CG-791, [redacted], USCG | 2 |
| 6 | 12 | “However, for the [redacted] production environment .. [redacted] | **Suggested revision:** Redact this sentence.<br>**Reasoning:** The inability to [redacted] | [redacted], CG-791, [redacted], USCG | 2 |

2

~~FOR OFFICIAL USE ONLY (FOUO)/CONTROLLED UNCLASSIFIED INFORMATION (CUI)~~

# (U) Deputy Assistant Commandant for Resources (cont'd)



~~FOR OFFICIAL USE ONLY (FOUO)/CONTROLLED UNCLASSIFIED INFORMATION (CUI)~~

| Comment Number | Report Page | Line or Bullet | Comments | Component /Point of Contact | Type |
|---|---|---|---|---|---|
| | | [redacted] [redacted]” | [redacted]<br>**CUI Category:** CUI//PHYS; Physical Security - Homeland | | |
| 7 | 13 | Figure 1. Lever Door Lock at the Production Environment Server Room | **Suggested revision:** Redact, crop, or mark the photo as CUI.<br>**Reasoning:** A photo may provide [redacted]<br>**CUI Category:** Physical Security – Homeland | [redacted], CG-791, [redacted] USCG | 2 |
| 8 | 14 | “Instead… available on [redacted] that could be unavailable during a disruptive event.” | **Suggested revision:** Either redact the entire sentence or remove ‘[redacted]’<br>**New language:** “Instead, the System's procedures were available on [redacted] that could be unavailable during a disruptive event.”<br>**CUI Category:** ISVI; Physical Security - Homeland | [redacted], CG-791, [redacted], USCG | 2 |
| 9 | 29 | “We identified [redacted] unclassified Coast Guard information systems… From the [redacted] systems …and [redacted] systems for review.” | **Suggested revision:** Remove ‘[redacted]’ from both sentences and add “identified” to the second sentence.<br>**New language:** “We identified unclassified Coast Guard information systems operating on the DODIN as of June 2021 and obtained information on the overall risks for these systems from the enterprise Mission Assurance Support Service system.48 From the systems identified, we nonstatistically selected the [redacted] systems for review.”<br>**Reasoning:** This information is not public knowledge and was derived from a CUI internal system. | [redacted], CG-791, [redacted] USCG | 2; 4 |
| | | | Cleared without comments. | [redacted], CUOPS Director, CGCC-33, [redacted], USCG | |
| | | | Cleared without comments. | [redacted], Senior Information Security Officer, CG-62, [redacted], USCG | |

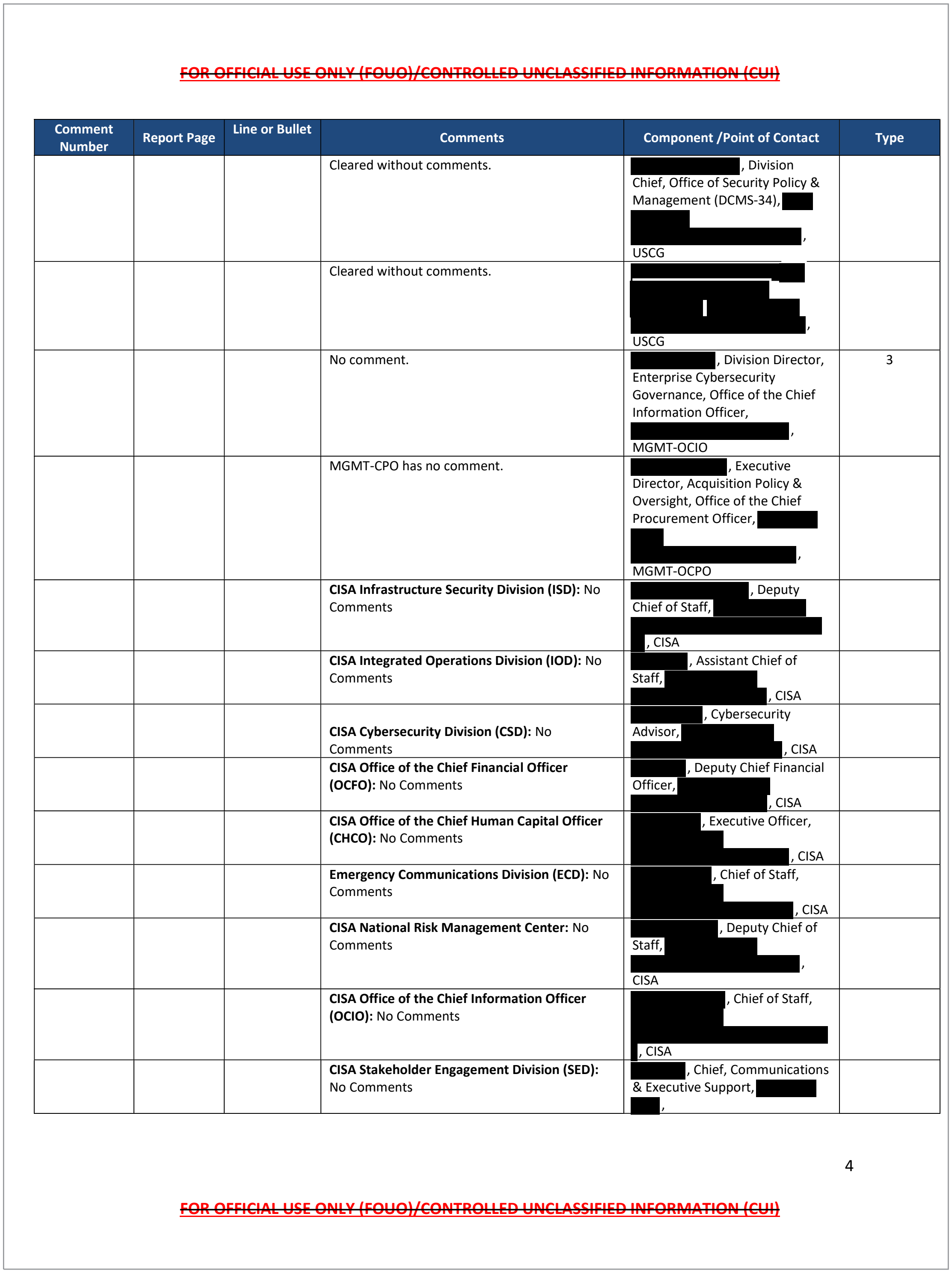
3

~~FOR OFFICIAL USE ONLY (FOUO)/CONTROLLED UNCLASSIFIED INFORMATION (CUI)~~

**Final Report Reference**

**Page 38**

# (U) Deputy Assistant Commandant for Resources (cont'd)



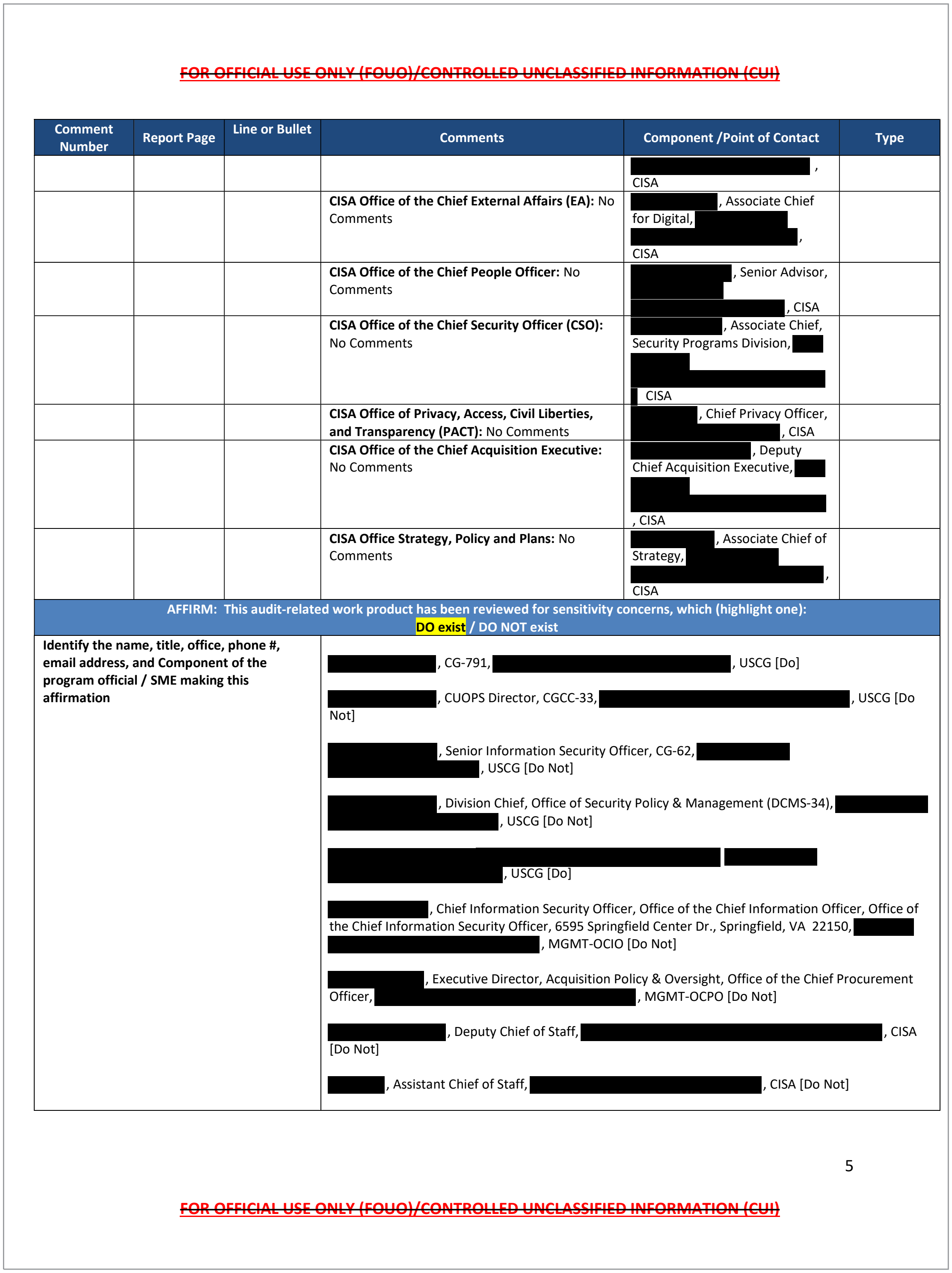
~~FOR OFFICIAL USE ONLY (FOUO)/CONTROLLED UNCLASSIFIED INFORMATION (CUI)~~

| Comment Number | Report Page | Line or Bullet | Comments | Component /Point of Contact | Type |
|---|---|---|---|---|---|
| | | | Cleared without comments. | [redacted], Division Chief, Office of Security Policy & Management (DCMS-34), [redacted], USCG | |
| | | | Cleared without comments. | [redacted], USCG | |
| | | | No comment. | [redacted], Division Director, Enterprise Cybersecurity Governance, Office of the Chief Information Officer, [redacted], MGMT-OCIO | 3 |
| | | | MGMT-CPO has no comment. | [redacted], Executive Director, Acquisition Policy & Oversight, Office of the Chief Procurement Officer, [redacted], MGMT-OCPO | |
| | | | **CISA Infrastructure Security Division (ISD):** No Comments | [redacted], Deputy Chief of Staff, [redacted], CISA | |
| | | | **CISA Integrated Operations Division (IOD):** No Comments | [redacted], Assistant Chief of Staff, [redacted], CISA | |
| | | | **CISA Cybersecurity Division (CSD):** No Comments | [redacted], Cybersecurity Advisor, [redacted], CISA | |
| | | | **CISA Office of the Chief Financial Officer (OCFO):** No Comments | [redacted], Deputy Chief Financial Officer, [redacted], CISA | |
| | | | **CISA Office of the Chief Human Capital Officer (CHCO):** No Comments | [redacted], Executive Officer, [redacted], CISA | |
| | | | **Emergency Communications Division (ECD):** No Comments | [redacted], Chief of Staff, [redacted], CISA | |
| | | | **CISA National Risk Management Center:** No Comments | [redacted], Deputy Chief of Staff, [redacted], CISA | |
| | | | **CISA Office of the Chief Information Officer (OCIO):** No Comments | [redacted], Chief of Staff, [redacted], CISA | |
| | | | **CISA Stakeholder Engagement Division (SED):** No Comments | [redacted], Chief, Communications & Executive Support, [redacted], | |

4

~~FOR OFFICIAL USE ONLY (FOUO)/CONTROLLED UNCLASSIFIED INFORMATION (CUI)~~

# (U) Deputy Assistant Commandant for Resources (cont'd)



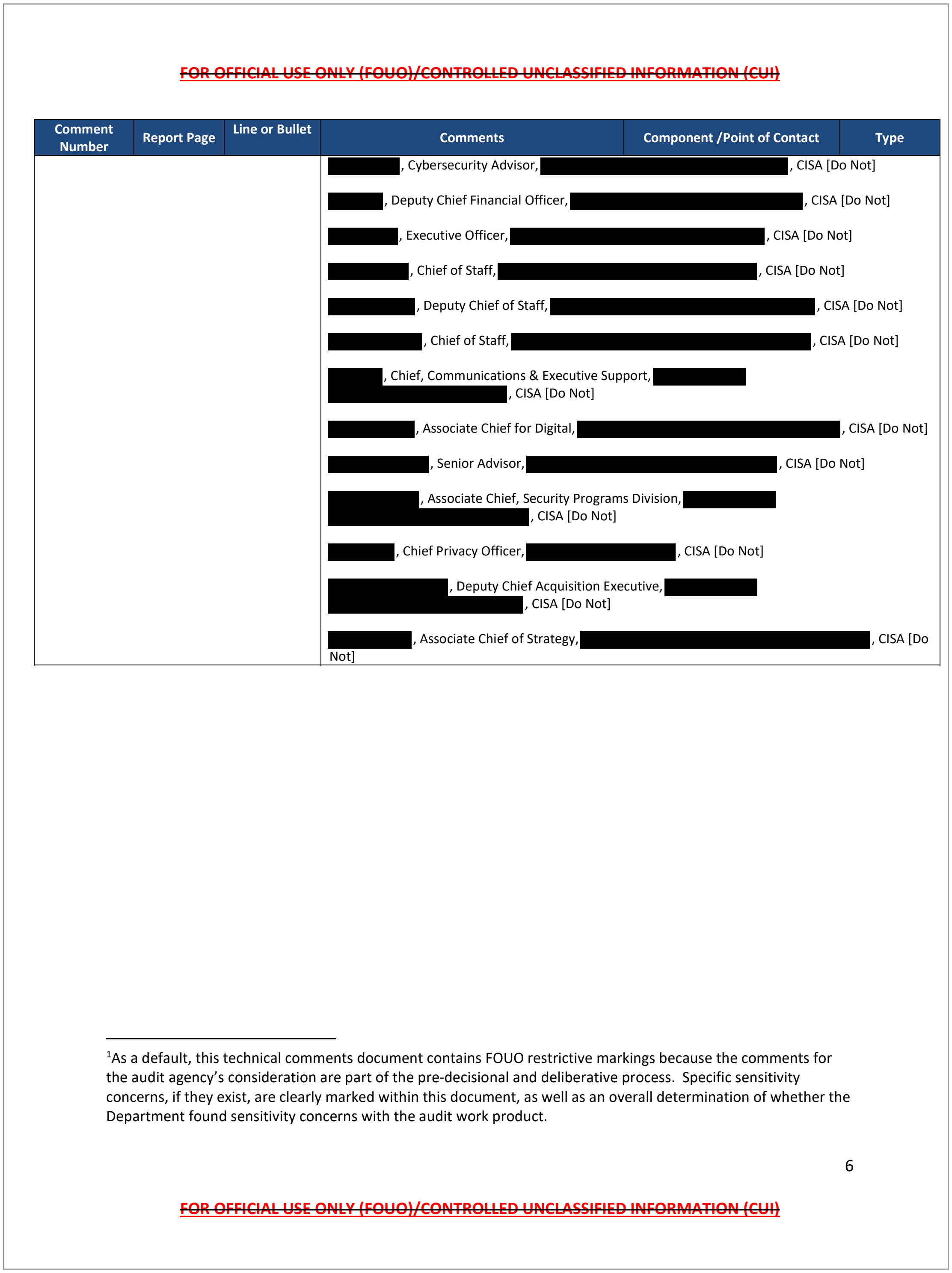
~~FOR OFFICIAL USE ONLY (FOUO)/CONTROLLED UNCLASSIFIED INFORMATION (CUI)~~

| Comment Number | Report Page | Line or Bullet | Comments | Component /Point of Contact | Type |
|---|---|---|---|---|---|
| | | | | [redacted] , CISA | |
| | | | **CISA Office of the Chief External Affairs (EA):** No Comments | [redacted], Associate Chief for Digital, [redacted], CISA | |
| | | | **CISA Office of the Chief People Officer:** No Comments | [redacted], Senior Advisor, [redacted], CISA | |
| | | | **CISA Office of the Chief Security Officer (CSO):** No Comments | [redacted], Associate Chief, Security Programs Division, [redacted] CISA | |
| | | | **CISA Office of Privacy, Access, Civil Liberties, and Transparency (PACT):** No Comments | [redacted], Chief Privacy Officer, [redacted], CISA | |
| | | | **CISA Office of the Chief Acquisition Executive:** No Comments | [redacted], Deputy Chief Acquisition Executive, [redacted], CISA | |
| | | | **CISA Office Strategy, Policy and Plans:** No Comments | [redacted], Associate Chief of Strategy, [redacted], CISA | |
| **AFFIRM: This audit-related work product has been reviewed for sensitivity concerns, which (highlight one): DO exist / DO NOT exist** | | | | | |
| **Identify the name, title, office, phone #, email address, and Component of the program official / SME making this affirmation** | | | [redacted], CG-791, [redacted], USCG [Do]<br>[redacted], CUOPS Director, CGCC-33, [redacted], USCG [Do Not]<br>[redacted], Senior Information Security Officer, CG-62, [redacted], USCG [Do Not]<br>[redacted], Division Chief, Office of Security Policy & Management (DCMS-34), [redacted], USCG [Do Not]<br>[redacted] [redacted], USCG [Do]<br>[redacted], Chief Information Security Officer, Office of the Chief Information Officer, Office of the Chief Information Security Officer, 6595 Springfield Center Dr., Springfield, VA 22150, [redacted], MGMT-OCIO [Do Not]<br>[redacted], Executive Director, Acquisition Policy & Oversight, Office of the Chief Procurement Officer, [redacted], MGMT-OCPO [Do Not]<br>[redacted], Deputy Chief of Staff, [redacted], CISA [Do Not]<br>[redacted], Assistant Chief of Staff, [redacted], CISA [Do Not] | | |

5

~~FOR OFFICIAL USE ONLY (FOUO)/CONTROLLED UNCLASSIFIED INFORMATION (CUI)~~

# (U) Deputy Assistant Commandant for Resources (cont'd)



~~FOR OFFICIAL USE ONLY (FOUO)/CONTROLLED UNCLASSIFIED INFORMATION (CUI)~~

| Comment Number | Report Page | Line or Bullet | Comments | Component /Point of Contact | Type |
|---|---|---|---|---|---|
| | | | [redacted], Cybersecurity Advisor, [redacted], CISA [Do Not]<br>[redacted], Deputy Chief Financial Officer, [redacted], CISA [Do Not]<br>[redacted], Executive Officer, [redacted], CISA [Do Not]<br>[redacted], Chief of Staff, [redacted], CISA [Do Not]<br>[redacted], Deputy Chief of Staff, [redacted], CISA [Do Not]<br>[redacted], Chief of Staff, [redacted], CISA [Do Not]<br>[redacted], Chief, Communications & Executive Support, [redacted], CISA [Do Not]<br>[redacted], Associate Chief for Digital, [redacted], CISA [Do Not]<br>[redacted], Senior Advisor, [redacted], CISA [Do Not]<br>[redacted], Associate Chief, Security Programs Division, [redacted], CISA [Do Not]<br>[redacted], Chief Privacy Officer, [redacted], CISA [Do Not]<br>[redacted], Deputy Chief Acquisition Executive, [redacted], CISA [Do Not]<br>[redacted], Associate Chief of Strategy, [redacted], CISA [Do Not] | | |

[1] As a default, this technical comments document contains FOUO restrictive markings because the comments for the audit agency's consideration are part of the pre-decisional and deliberative process. Specific sensitivity concerns, if they exist, are clearly marked within this document, as well as an overall determination of whether the Department found sensitivity concerns with the audit work product.

6

~~FOR OFFICIAL USE ONLY (FOUO)/CONTROLLED UNCLASSIFIED INFORMATION (CUI)~~

# (U) Acronyms and Abbreviations

| | |
|---|---|
| ~~(CUI)~~<br>**(U) ATO** | Authorization to Operate |
| **(U) C5ISC** | Command, Control, Communications, Computer, Cyber, and Intelligence Service Center |
| **(U) CGCYBER** | Coast Guard Cyber Command |
| **(U) CIO** | Chief Information Officer |
| **(U) CJCS** | Chairman of the Joint Chiefs of Staff |
| **(U) DHS** | Department of Homeland Security |
| **(U) DoD** | Department of Defense |
| **(U) DODIN** | Department of Defense Information Network |
| **(U) eMASS** | enterprise Mission Assurance Support Service |
| **(U) ISSM** | Information Systems Security Manager |
| **(U) ISSO** | Information Systems Security Officer |
| **~~(CUI)~~** [redacted] | [redacted] |
| **(U) NIST** | National Institute of Standards and Technology |
| **(U) POA&M** | Plan of Action and Milestones |
| **(U) RMF** | Risk Management Framework |
| **~~(CUI)~~** [redacted] | [redacted] |
| **(U) SCA** | Security Control Assessor |
| **(U) SISO** | Senior Information Security Officer |
| **(U) STIG** | Security Technical Implementation Guide |
| **~~(CUI)~~** [redacted] | [redacted] |
| **(U) USCYBERCOM** | U.S. Cyber Command |
| **~~(CUI)~~** [redacted] | [redacted] |
| **~~(CUI)~~** [redacted] | [redacted]<br>**~~(CUI)~~** |

## U.S. Department of Defense
## Whistleblower Protection

*Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-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/

𝕏
www.twitter.com/DoD_IG

**LinkedIn**
www.linkedin.com/company/dod-inspector-general/

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

## U.S. Department of Homeland Security

*To view this and any other DHS OIG reports, please visit our website: www.oig.dhs.gov*

*For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov*

*To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline*

*If you cannot access our website, please contact the hotline by phone or mail:*

*Call: 1.800.323.8603*

*U.S. Mail:*
*Department of Homeland Security*
*Office of Inspector General*
*Attention: Hotline*
*245 Murray Drive SW, Mail Stop 0305*
*Washington, DC 20528-0305*

***U.S. Department of Defense***
***Office of Inspector General***

4800 Mark Center Drive
Alexandria, Virginia 22350-1500

www.dodig.mil
DoD Hotline 1.800.424.9098

***U.S. Department of Homeland Security***
***Office of Inspector General***

245 Murray Drive SW, Mail Stop 0305
Washington, DC 20528-0305

www.oig.dhs.gov
DHS OIG Hotline 1.800.323.8603