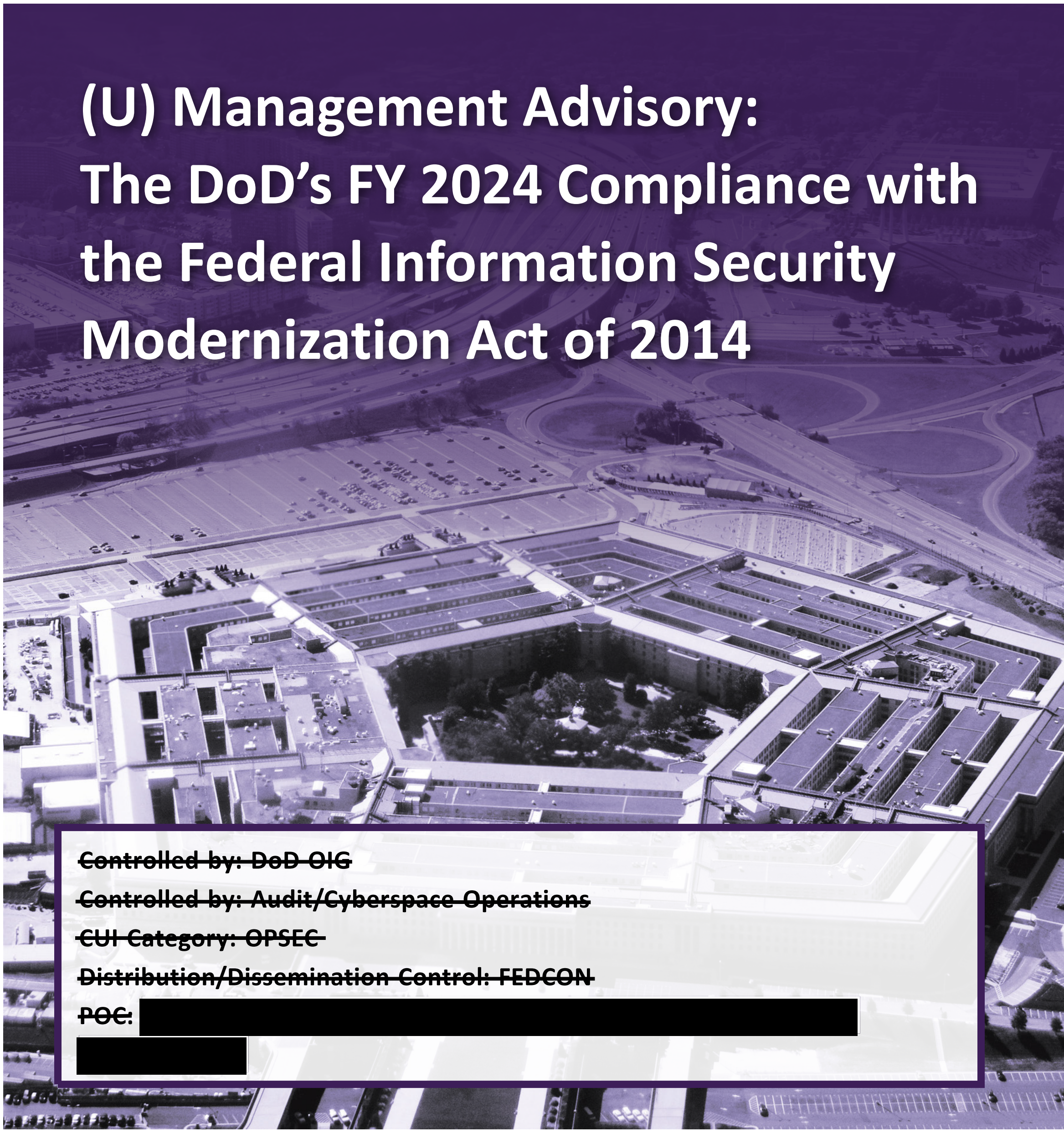
Report No. DODIG-2025-086

~~CUI~~

Inspector General

U.S. Department of Defense

APRIL 16, 2025



(U) Management Advisory: The DoD's FY 2024 Compliance with the Federal Information Security Modernization Act of 2014

~~Controlled by: DoD OIG~~

~~Controlled by: Audit/Cyberspace Operations~~

~~CUI Category: OPSEC~~

~~Distribution/Dissemination Control: FEDCON~~

~~POC:~~ [redacted]

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

~~CUI~~

INSPECTOR GENERAL

INTEGRITY

EFFICIENCY

DEPARTMENT OF DEFENSE

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

April 16, 2025

MEMORANDUM FOR CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
COMMANDANT OF THE COAST GUARD
DIRECTOR, DEFENSE SECURITY COOPERATION AGENCY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

SUBJECT: (U) Management Advisory: The DoD's FY 2024 Compliance with the Federal Information Security Modernization Act of 2014 (Report No. DODIG-2025-086)

(U) This management advisory provides recommendations related to the DoD Office of Inspector General's review of the DoD's compliance with the Federal Information Security Modernization Act of 2014 (FISMA), which we announced on December 11, 2023 (Project No. D2024-D000CP-0043.000). However, the results in this management advisory do not fully represent all the requirements for each metric or the DoD's overall FISMA rating. We conducted work on this management advisory from December 2023 through January 2025 with integrity, objectivity, and independence, as required by the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Federal Offices of Inspector General.

(U) We provided the draft management advisory to the DoD Chief Information Officer (CIO) and requested written comments on the recommendations. We considered the DoD CIO's comments on the draft when preparing the final advisory. These comments are included in the advisory.

(U) This management advisory contains 12 recommendations that we consider resolved but open. We will close the recommendations when management provides us documentation showing that all agreed-upon actions to implement the recommendations are completed.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. Therefore, within 90 days please provide us documentation showing you have completed the agreed-upon actions. Send your response as a PDF file to either [redacted] if unclassified or [redacted] if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

(U) If you have any questions, please contact me at [redacted] We appreciate the cooperation and assistance received during the review.

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

(U) Executive Summary

(U) This management advisory provides recommendations related to the DoD Office of Inspector General's review of the DoD's compliance with the Federal Information Security Modernization Act of 2014 (FISMA), which we announced on December 11, 2023 (Project No. D2024-D000CP-0043.000). However, the results in this management advisory do not fully represent all the requirements for each metric or the DoD's overall FISMA rating.[1]

(U) FISMA requires senior agency officials to provide security for the information and information systems (information security program) that support the operations and assets under their control. FISMA also requires Federal agencies to conduct an annual, independent review of the effectiveness of their information security program and practices. For a Federal agency with an Inspector General (IG) appointed under the IG Act of 1978, that IG, or an independent external auditor designated by that IG, must conduct the review and submit the results to the Office of Management and Budget (OMB) and Department of Homeland Security (DHS).

(U) Although the DoD generally had information security-related policies and procedures in place for the 12 IG FISMA metrics that we are reporting on, DoD officials did not consistently comply with OMB, the National Institute of Standards and Technology (NIST), or DoD guidance when implementing those policies and procedures.[2] Specifically, DoD officials did not consistently:

- (U) collect self-attestations from third-party software providers;
- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]

(U) Consistent implementation of cybersecurity policies and procedures is critical for an effective cybersecurity program and reduces the risk of successful cyber attacks, data breaches, data loss, data manipulation, and unauthorized disclosures of mission-essential or sensitive information by malicious actors.

(U) To address the issues identified in this management advisory, we made 12 recommendations to the DoD Chief Information Officer (CIO) to direct the DoD Components to identify all critical and non-critical third-party software used, collect self-attestations from third-party software providers, and ensure that the DoD Components are accurately reporting the system authorization status and implementing the necessary NIST controls for their information

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

[2] (U) Although we report on all required metrics each year, we used a risk-based approach for selecting the metrics to report on in this management advisory to ensure that we covered most FISMA functions and domains.

(U) systems. In response to this advisory, the official Performing the Duties of the DoD CIO agreed to take action to address the 12 recommendations. We consider the 12 recommendations resolved but open. Please see the Recommendations, Management Comments, and Our Response section for more details and the status of the recommendations.

~~(CUI)~~ Additionally, the DoD continued to have [redacted] from FY 2021 through FY 2024, which fluctuated between the [redacted] Although the DoD has taken steps to improve aspects of its information security program (FISMA), [redacted] See Figure 1 below for the DoD's overall FISMA rating for FY 2021 through FY 2024 and how it relates to an effective level as defined by the annual IG FISMA reporting metrics guidance.

(U) Figure 1. FY 2021 Through FY 2024 DoD Overall FISMA Ratings

[redacted]

(U) Source: The DoD OIG.

(U) Introduction

(U) Background

(U) On December 17, 2002, the President signed the "Federal Information Security Management Act" into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). The law provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and provides a mechanism for improved oversight of Federal agency information security programs. Congress amended the law on December 18, 2014, (Public Law 113-283) and renamed it the "Federal Information Security Modernization Act of 2014 [FISMA]." The amendment also establishes the Director of the OMB's authority to oversee information security policies and practices for Federal agencies and the Secretary of the Department of Homeland Security's authority to manage the information security policies and practices across the Government.

(U) FISMA requires senior agency officials to provide security for the information and information systems (information security program) that support the operations and assets under their control, including assessing the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems. Federal agencies' information security programs are supported by security policy issued through the OMB, DHS, and risk-based standards and guidelines published by NIST.[3]

(U) FISMA also requires Federal agencies to conduct an annual, independent review of the effectiveness of their information security program and practices. For a Federal agency with an IG appointed under the IG Act of 1978, that IG, or an independent external auditor designated by that IG, must conduct the review and submit the results to the OMB and DHS. Each year, the OMB issues guidance that requires the IGs to assess the effectiveness of their agencies' information security program using annual IG FISMA reporting metrics.[4] The OMB, DHS, and Council of the Inspectors General on Integrity and Efficiency develop the IG FISMA reporting metrics, in consultation with the Federal CIO Council.

[3] (U) This report contains information that has been redacted because the DoD identified it as Controlled Unclassified Information (CUI) that is not releasable to the public. CUI is Government-created or owned unclassified information that allows for, or requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies.

[4] (U) For FY 2024 FISMA guidance, the OMB issued Memorandum M-24-04, "Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements," on December 4, 2023.

(U) FISMA Reporting Metrics

(U) The IG FISMA metrics are grouped into nine domains aligned under the five information security functions established by the NIST Cybersecurity Framework, Version 1.1: Identify, Protect, Detect, Respond, and Recover.[5] The NIST Cybersecurity Framework (CSF) provides Federal agencies with a common structure for identifying and managing cybersecurity risk across their information technology enterprise and IGs with guidance for assessing the maturity of the controls in place to address those risks.[6] Table 1 describes the nine FISMA domains by NIST CSF function.

(U) Table 1. Descriptions of NIST Cybersecurity Framework Functions and FISMA Domains

(U) Function	Domain	Description
Identify	Risk Management	Risk management is the program and processes for managing information security risks to organizational operations (including mission, functions, image, and reputation), organizational assets, staff, and other organizations.
	Supply Chain Risk Management (SCRM)	Supply chain risk management is the process of ensuring that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity requirements.
Protect	Configuration Management	Configuration management consists of a collection of activities focused on establishing and maintaining the integrity of information technology products and information systems.
	Identity and Access Management	Identity and access management consists of the controls and processes for identifying users, using credentials, and managing user access to network resources.
	Data Protection and Privacy	Data protection and privacy consists of the controls and processes for protecting systems and information (data) and ensuring that management of those systems and data are consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Security Training	Security training consists of an established program that ensures all users complete the necessary mandatory cybersecurity training requirements, including specialized training for individuals requiring privileged access.
Detect	Information Security Continuous Monitoring (ISCM)	ISCM is the process for maintaining ongoing awareness of information security, vulnerabilities, and threats to support operational risk management decisions. **(U)**

[5] (U) "FY 2023 – 2024 IG FISMA Reporting Metrics," February 10, 2023.

(U) NIST, "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.1, April 16, 2018. The NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems.

[6] (U) NIST defines a control as the safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information or ensure compliance with applicable privacy requirements and manage privacy risks. Controls can be used to demonstrate compliance with a variety of governmental, organizational, or institutional security and privacy requirements.

(U) Table 1. Descriptions of NIST Cybersecurity Framework Functions and FISMA Domains (cont'd)

(U) Function	Domain	Description
Respond	Incident Response	Incident response is a formal, focused, and coordinated approach to responding to cybersecurity incidents.
Recover	Contingency Planning	Contingency planning is a coordinated strategy involving plans, procedures, and technical measures that will enable the recovery of information systems, operations, and data after a disruption. **(U)**

(U) Source: The DoD OIG.

(U) The IG FISMA metrics use executive orders; OMB guidance; NIST guidance, such as NIST Special Publication (SP) 800-53, Revision 5 controls; and other Federal information security guidance as criteria for assessing the effectiveness of an agency's information security program and practices.[7]

(U) FISMA Reporting Metric Updates

(U) In FY 2021, the OMB required IGs to report annually on 66 metrics. In FY 2022, the OMB made significant changes to the FISMA oversight process and metric collection in support of Executive Order 14028 and encouraged agencies to shift toward a continuous assessment process.[8] For example, the OMB made the following changes to the IG FISMA reporting process in OMB Memorandum M-22-05.[9]

- (U) Transitioned the IG FISMA reporting metrics process to a multiyear cycle (2-year), which included a set of core metrics evaluated annually and the remaining supplemental metrics evaluated on a 2-year cycle beginning in FY 2023.
- (U) Established 20 core metrics that must be evaluated annually. These core metrics represent a combination of administration priorities, high-impact security processes, and essential functions to determine security program effectiveness, while the supplemental metrics represent important activities conducted by security programs.

[7] (U) NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5, updated December 2020.

[8] (U) Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021.

[9] (U) OMB Memorandum M-22-05, "Fiscal Year 2021 – 2022 Guidance on Federal Information Security and Privacy Management Requirements," December 6, 2021. IG FISMA metrics are questions addressing various aspects of an organization's information security program.

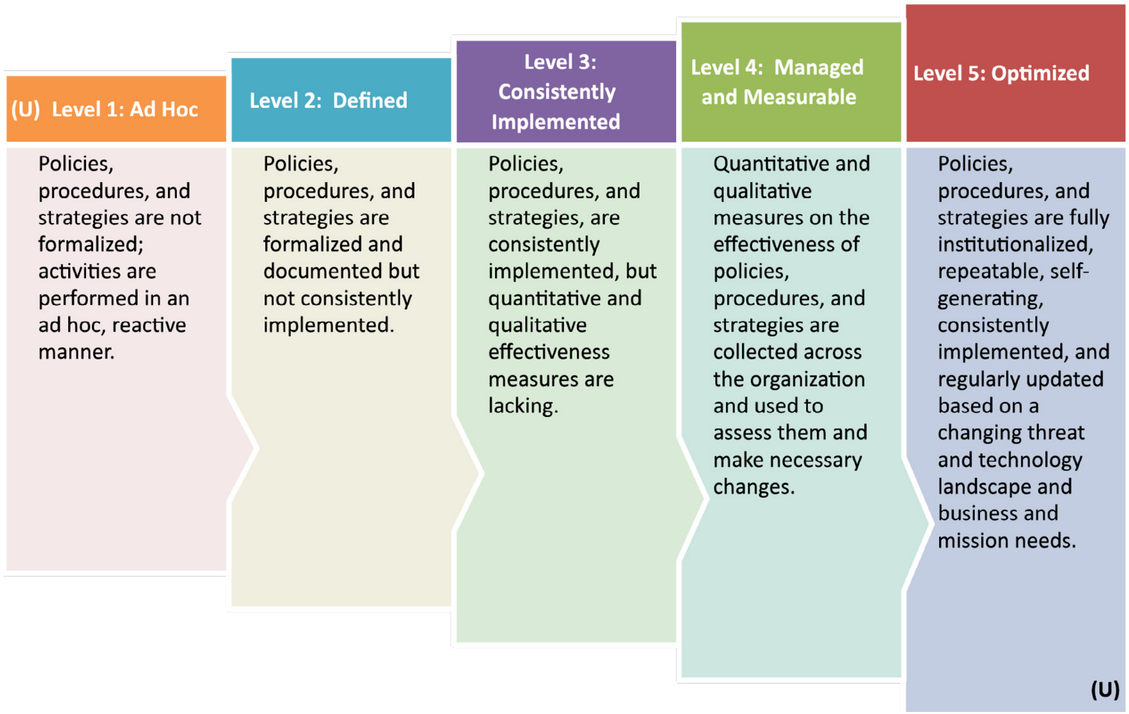
(U) As part of the new multiyear review cycle, IGs are required to report annually on the 20 core metrics and assess the remaining 37 supplemental metrics over a 2-year cycle.[10] FY 2023 was the first year of a 2-year cycle, and IGs were required to report on 40 metrics—20 core and 20 supplemental. The IGs reported on 37 metrics (20 core and 17 supplemental) in FY 2024.[11]

(U) FISMA Scoring

(U) The IGs assign a maturity level (rating) for each domain by determining whether the agency has issued policies and procedures that address specific NIST SP 800-53 controls and other Federal requirements applicable to the domain, and whether the policies and procedures are implemented and effective. The IG FISMA reporting metrics guidance requires IGs to use a five-level IG FISMA maturity model when determining the agency's level of effectiveness of security controls. Within the context of the maturity model, the foundational levels require agencies to develop sound policies and procedures, while advanced levels capture the extent to which agencies institutionalize those policies and procedures.

(U) Operating at the Managed and Measurable (Level 4) or higher is considered an effective level of security. Figure 2 shows the general five-level IG FISMA maturity model; however, each metric has its own scale tailored to the unique requirements for each question.

(U) Figure 2. IG FISMA Maturity Model



(U) Level 1: Ad Hoc

Policies, procedures, and strategies are not formalized; activities are performed in an ad hoc, reactive manner.

Level 2: Defined

Policies, procedures, and strategies are formalized and documented but not consistently implemented.

Level 3: Consistently Implemented

Policies, procedures, and strategies, are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.

Level 4: Managed and Measurable

Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.

Level 5: Optimized

Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business and mission needs.

(U)

(U) Source: FY 2023 – FY 2024 IG FISMA Reporting Metrics Guidance.

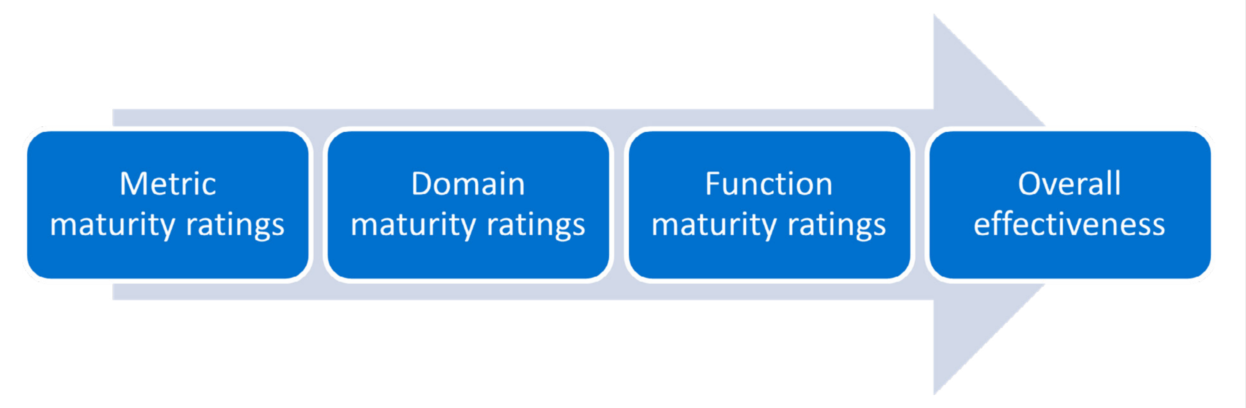
[10] (U) The FY 2023 – 2024 IG FISMA reporting metrics are based on the FY 2021 IG FISMA reporting metrics, which contained 66 total metric questions. There are 37 Supplement metrics after removing the 20 Core metrics and 9 summary metric questions. The summary metric questions are designed for IGs to report any issues or comments that were not included in the other metrics for each of the nine domains.

[11] (U) "FY 2023 – 2024 IG FISMA Reporting Metrics," February 10, 2023. The IG FISMA reporting metrics reference public law, Federal requirements, and NIST guidance as the criteria for measuring an agency's information security program and practices.

(U) Determining the agency's overall effectiveness as it pertains to FISMA is a multistep process. The IGs first assign a maturity level, a rating, for each domain based on the outcome of the core metrics, as they represent the administration priorities and other high-risk areas. The IGs then consider the domain maturity-level determinations when assigning a maturity level for each function. Lastly, the IGs use the corresponding function maturity-level determinations to determine the agency's overall effectiveness.

(U) For FY 2024, the IG FISMA reporting metrics guidance requires IGs to use a calculated average when determining the domain, function, and the overall program ratings. To provide greater flexibility to IGs and assist with rounding the calculated averages up or down, IGs may consider other data points and risk factors, such as the agency's unique missions, resources, and challenges and the results of the FY 2023 and FY 2024 Supplemental metrics, when determining the maturity levels for each domain and function. Figure 3 shows how the IGs determine the overall effectiveness for their respective agency's information security program.

(U) Figure 3. IG Process for Determining the Agency's Overall Effectiveness



Metric maturity ratings

Domain maturity ratings

Function maturity ratings

Overall effectiveness

(U) Source: FY 2023 – 2024 IG FISMA Reporting Metrics.

(U) DoD Roles and Responsibilities for the DoD Information Security Program

(U) DoD Instruction 8500.01 establishes the DoD cybersecurity program to protect and defend DoD information and information technology and permit DoD missions and operations to continue under any cyber situation or condition.[12] DoD Instruction 8510.01 establishes the cybersecurity Risk Management Framework (RMF) for DoD systems and designates NIST special publications as the authoritative guidelines.[13] As part of the DoD RMF process, the Instruction requires DoD Components, including the Coast Guard at all times even when it

[12] (U) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014 (Incorporating Change 1, October 7, 2019).

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

(U) is a Service in the Department of Homeland Security, to categorize systems and select controls in accordance with the Committee on National Security Systems (CNSS) Instruction 1253 and implement a corresponding set of controls in accordance with NIST SP 800-53.[14]

(U) The CNSS Instruction 1253 identifies applicable NIST SP 800-53 system baseline controls while NIST SP 800-53 provides a catalog of security and privacy controls for information systems and organizations to implement as part of an organization-wide process to manage risk. DoD Instruction 8510.01 also requires DoD Components to assess their system controls to determine that they are correctly implemented, operating as intended, and producing the desired outcomes.

(U) Additionally, all DoD information technology is assigned to and governed by a DoD Component cybersecurity program that manages risk commensurate with the importance of supported missions and the value of potentially affected information or assets. DoD guidance defines the following roles and responsibilities pertaining to cybersecurity.

(U) Authorizing Official

(U) Authorizing officials (AOs) make authorization decisions for information technology systems, which is also known as the authorization to operate (ATO) process. AOs grant an ATO after determining whether the overall risks of operating a system are at an acceptable level to support mission requirements. In addition, AOs are responsible for monitoring the information system vulnerabilities and mitigating identified vulnerabilities using plans of action and milestones.

(U) Chief Information Officer

(U) The DoD CIO monitors, evaluates, and provides advice to the Secretary of Defense for all DoD cybersecurity activities and develops and establishes DoD cybersecurity policy and guidance. The DoD CIO must also appoint a DoD Senior Information Security Officer (SISO). The DoD Component CIOs, for the respective DoD Component heads, develop, implement, maintain, and enforce a DoD Component cybersecurity program and appoint DoD Component Chief Information Security Officers (CISOs) to direct and coordinate the DoD Component cybersecurity program.

(U) Senior Information Security Officer

(U) The DoD SISO, for the DoD CIO, directs and coordinates the DoD cybersecurity program, such as developing and maintaining cybersecurity program policies, verifying implementation of established policies and procedures, and collecting cybersecurity metrics. The DoD Component CISOs direct and coordinate the DoD Component cybersecurity program.

[14] (U) CNSS Instruction 1253, "Categorization and Control Selection for National Security Systems," July 29, 2022.

(U) A national security system is an information system: (1) in which the function, operation, or use involves intelligence activities, cryptologic activities related to national security, command and control of military forces, weapon or weapons system equipment, or the direct fulfillment of military or intelligence missions; or (2) is protected by executive order or act of Congress in the interest of national security or foreign policy. A non-national security system is any system that is not categorized as a national security system.

(U) The DoD Did Not Consistently Implement Aspects of Its DoD Information Security Program

(U) Although the DoD generally had information security-related policies and procedures in place for the 12 IG FISMA metrics that we are reporting on, DoD officials did not consistently comply with OMB, NIST, or DoD guidance when implementing those policies and procedures. See Appendix A for details about the 12 metrics. Specifically, DoD officials did not consistently:

- (U) collect self-attestations from third-party software providers certifying that they used NIST secure development practices as required by OMB guidance for software used on the DoD Information Network (DODIN) (Metrics 3 and 14);
- ~~(CUI)~~ report the [redacted] for their non-national security systems as required by DoD guidance [redacted] or
- ~~(CUI)~~ implement or report that they implemented [redacted] for their systems as required by NIST and DoD guidance [redacted]

(U) Consistent implementation of cybersecurity policies and procedures is critical for an effective cybersecurity program and reduces the risk of successful cyber attacks, data breaches, data loss, data manipulation, and unauthorized disclosures of mission-essential or sensitive information by malicious actors. Therefore, the DoD should take action to address the recommendations in this management advisory, which will result in more consistent implementation of its information security-related policies and procedures and assist with reducing the associated cybersecurity risks.

~~(CUI)~~ Additionally, the DoD continued to have an [redacted] program from FY 2021 through FY 2024 as defined by the IG FISMA reporting metric guidance, [redacted] Although the DoD has taken steps to improve aspects of its information security program, [redacted] In addition, officials need [redacted] Therefore, the DoD is [redacted]

(U) Risk Management and SCRM Domains

(U) DoD Officials Did Not Consistently Collect Self-Attestations from Third-Party Software Providers

(U) DoD Components did not consistently collect self-attestations from third-party software providers to certify that they used NIST secure development practices for software used on the DODIN as required by OMB guidance (Metrics 3 and 14). Software providers submit self-attestations to an agency that uses their software and serves as an affirmative statement certifying that the provider followed the NIST secure software development requirements.

(U) The NIST requirements include several best practices regarding how software developers should address and maintain the security of code. In addition, the IG FISMA reporting metrics guidance references Executive Order 14028 and OMB Memorandum M-22-18 that require the third-party software attestations as part of Federal agencies' processes for maintaining software inventories and managing supply chain cybersecurity risks for products and services from third-party providers.

(U) In May 2021, the President issued Executive Order 14028 directing NIST to issue guidance that identifies practices to enhance security of the software supply chain and the OMB to require that agencies comply with guidelines issued by NIST. In response to the Executive Order, NIST issued its Secure Software Development framework to serve as a core set of high-level secure software development practices that can be integrated into the software development lifecycle.[15] The framework is designed to reduce the number of vulnerabilities and the potential impact of the exploitation of undetected or unaddressed vulnerabilities in released software and address the root causes of vulnerabilities to prevent future recurrences.

(U) In September 2022, the OMB issued Memorandum M-22-18, as amended by OMB Memorandum M-23-16, requiring Federal agencies to obtain a self-attestation from software providers before using any third-party software.[16] The self-attestations serve as a conformance statement made by software providers certifying that they followed NIST software development guidance for third-party software that deploys continuous updates or that they developed or significantly modified their software after September 2022. OMB Memorandum M-22-18, as amended by OMB Memorandum M-23-16, requires agencies to collect the self-attestations from third-party providers for critical software by June 2024 and September 2024 for non-critical software. Agencies can seek an extension from the OMB, but they must include a plan for meeting the underlying requirements.

~~(CUI)~~ To determine whether DoD Office of the CIO (OCIO) officials obtained all necessary self-attestations from third-party providers for critical and non-critical software used on the DODIN, we requested the complete DoD inventory of critical and non-critical third-party

[15] (U) NIST SP 800-218, "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities," February 2022.

[16] (U) OMB Memorandum M-23-16, "Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices," June 9, 2023.

~~(CUI)~~ software subject to the attestation requirement and self-attestations collected from third-party software providers. As of October 2024, DoD OCIO officials reported that they did not have a complete inventory of all critical and non-critical third-party software but estimated that the DoD had [redacted] instances of third-party software. Of the [redacted] instances of third-party software, DoD OCIO officials reported that they had [redacted] self-attestations from third-party providers. In addition, DoD OCIO officials stated that they did not have an estimated completion date to obtain the remaining third-party software attestations in accordance with OMB requirements.

~~(CUI)~~ Without identifying all third-party software used by the DoD or collecting the required self-attestations from third-party software providers in a timely manner, [redacted] Therefore, the DoD CIO should direct DoD Components, including the Coast Guard, in coordination with their CISOs, CIOs, and AOs, to:

- (U) identify all critical and non-critical software on the DODIN that is subject to OMB-required self-attestation requirements;
- (U) obtain OMB-required self-attestations from software providers or implement an OMB-approved alternative solution for all identified third-party software on the DODIN; and
- (U) establish a plan of action and milestones to obtain all remaining OMB-required third-party provider self-attestations and request an extension from the OMB deadline.

(U) Information Security Continuous Monitoring Domain

~~(CUI)~~ [redacted]

~~(CUI)~~ The DoD Components [redacted] as required by DoD guidance in an accurate manner for their non-national security systems [redacted] For example, DoD Components [redacted][17]

cATOs are a modernized authorization process designed to work with software delivery organizations that want to provide the ability to deploy software more rapidly, while improving security.

[17] (U) eMASS is a tool that captures key information system documentation from the DoD RMF process, such as system security plans, security control test results, plans of action and milestones, and authorization decisions.

(U) An ATO is an official management decision made by an AO to operate an information system and explicitly accept the associated risk based on implementation of a set of security and privacy controls. All DoD systems must be reauthorized at least once every 3 years.

(U) cATOs have transitioned from the traditional ATO process, which is a document-based, point-in-time security assessment approach, toward a continuous risk determination and authorization concept that is accomplished by continuously assessing, monitoring, and managing risk. In contrast, a traditional ATO process does not support real-time data analytics for reporting security events, which is essential to supporting continuous monitoring and achieving the level of cybersecurity required to prevent today's cyber threats to the DODIN.

(U) In February 2022, the DoD SISO issued a memorandum stating that the DoD will begin transitioning traditional ATOs to cATOs for select systems.[18] The memorandum requires that DoD Components obtain approval from the DoD SISO before transitioning a system from ATO to a cATO. According to the memorandum, approval will be based on the DoD Component's ability to demonstrate key system capabilities, such as having robust continuous monitoring of RMF controls, conducting active cyber defense, and using the DoD's software development requirements and secure supply chain principles. In 2024, the DoD CIO issued cATO implementation guidance and evaluation criteria for DoD Components to follow when developing software and transitioning a system's ATO to a cATO.[19]

~~(CUI)~~ To determine whether the DoD Components correctly reported the system authorization status for non-national security systems, we reviewed the eMASS to identify whether DoD officials reported that their systems had a cATO, including those systems labeled as "continuous monitoring" or "ongoing authorizations." As a result, we identified the following [redacted] non-national security systems that officials reported as having a cATO in eMASS from March to August 2024.[20]

- ~~(CUI)~~ The Army reported [redacted]
- ~~(CUI)~~ The Navy reported [redacted]
- ~~(CUI)~~ The Air Force reported [redacted]
- ~~(CUI)~~ The Coast Guard reported [redacted] [21]
- ~~(CUI)~~ The Defense Security Cooperation Agency reported [redacted]

[18] (U) DoD SISO Memorandum, "Continuous Authorization to Operate (cATO)," February 2, 2022.

[19] (U) DoD CIO, "DevSecOps Continuous Authorization Implementation Guide," Version 1.0, March 21, 2024.

(U) DoD CIO, "DevSecOps Continuous Authorization to Operate (cATO) Evaluation Criteria," May 30, 2024.

[20] (U) We reviewed non-national security systems from eMASS because NIST SP 800-53 applies only to non-national security systems.

(U) The Army categorized the cATOs as "continuous monitoring," while the Navy, Air Force, Coast Guard, and Defense Security Cooperation Agency used "ongoing authorizations."

[21] (U) The Coast Guard is one of the six U.S. Military Services. During peacetime, the Coast Guard operates as a component of the Department of Homeland Security to enforce the Nation's laws at sea and protect the U.S. coastline, inland waterways, and ports. During wartime or at the President's direction, the Coast Guard serves as a part of the Navy. Therefore, the Coast Guard must comply with DoD cybersecurity requirements at all times 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.

~~(CUI)~~ Additionally, to verify that the DoD Components received the DoD SISO's approval before transitioning the [redacted] system authorizations from an ATO to a cATO, we requested a list of approved systems from DoD OCIO officials and asked the DoD Components whether they had approval to transition their systems. As of September 2024, DoD OCIO officials stated that the DoD SISO had not approved any systems to transition from an ATO to a cATO. When asked about having DoD SISO approval to transition their systems to a cATO, the DoD Components stated that [redacted] of the reported systems had approval and that they miscategorized the systems in eMASS. For example, Army officials stated that [redacted] of their systems were using cATOs and that they reported the system authorization status as "continuous monitoring" because they were renewing the ATOs on an annual basis to ensure that continuous monitoring was occurring. As of October 2024, the Navy, Coast Guard, and the Defense Security Cooperation Agency officials updated the system authorization status in eMASS, but the Army and the Air Force did not.

(U) Without accurately reporting system information in eMASS, or an equivalent system, the DoD does not have assurance that DoD Components, including the Coast Guard, are effectively managing risks or demonstrating that they have the necessary capabilities to reduce risk to an acceptable level in accordance with DoD guidance.[22] Therefore, the DoD CIO should direct the Army, Navy, Air Force, Coast Guard, and Defense Security Cooperation Agency CIOs, in coordination with their CISOs and AOs, to review eMASS, or an equivalent system, to ensure that officials are correctly reporting the system authorization status for their non-national security systems and update the status for any miscategorized systems. The DoD CIO should also direct DoD Components, including the Coast Guard, in coordination with their CISOs, CIOs, and AOs, to implement a process, such as periodic reviews of eMASS, or an equivalent system, to ensure that officials are accurately reporting the system authorization status for their non-national security systems in accordance with DoD guidance.

(U) DoD Information System Control Implementation

(U) DoD Officials Did Not Implement or Report That They Implemented All Necessary NIST Information System Controls

~~(CUI)~~ DoD Officials did not implement or report that they implemented all necessary information system controls for its non-national security systems as required by NIST and DoD guidance [redacted] For example, DoD Components reported that they did not implement [redacted] NIST SP 800-53 controls reviewed for their

[22] (U) For example, we reported in Report No. DODIG-2025-066, "Joint Audit of Security Controls over Coast Guard Systems Operating on the Department of Defense Information Network," February 7, 2025, that the Coast Guard did not consistently implement the cybersecurity controls reviewed to protect its systems operating on the DODIN in accordance with applicable cybersecurity requirements for the three systems reviewed.

~~(CUI)~~ non-national security systems that were associated with 9 IG FISMA metrics.[23] The nine IG FISMA metrics were from the Protect function (Configuration Management, Identity and Access Management, and Data Protection and Privacy domains) and the Recover function (Contingency Planning domain). See Appendix B for a description of the 9 IG FISMA metrics and the [redacted] associated NIST SP 800-53 information system controls that the DoD Components reported as not being implemented for their non-national security systems.

(U) DoD Instruction 8510.01 requires DoD Components to categorize systems and select controls in accordance with the CNSS Instruction 1253 and implement a corresponding set of controls in accordance with NIST SP 800-53, which provides a catalog of security and privacy controls for non-national security systems. The CNSS Instruction 1253 identifies applicable NIST SP 800-53 system baseline controls for organizations to implement as part of an organization-wide process to manage risk. DoD Components are required to track the implementation of the NIST controls for their information systems in their DoD RMF tool, such as eMASS. In addition, DoD Instruction 8500.01 requires DoD Component heads to ensure that all information technology under their purview complies with DoD guidance and that all systems are reported in eMASS or an equivalent system.

~~(CUI)~~ In 2024, the DoD OCIO officials started the [redacted], which is part of the DoD's enterprise-wide Cybersecurity Framework program. The DoD OCIO officials designed the [redacted] to monitor the DoD Components' implementation of the NIST information system controls associated with the 20 IG FISMA Core metrics and improve the overall DoD FISMA rating. DoD OCIO officials track the DoD Components' progress in eMASS, or an equivalent system.

~~(CUI)~~ To determine whether the DoD Components reported that they implemented the [redacted] associated NIST information system controls for the 37 FY 2024 Core and Supplemental metrics, we reviewed eMASS data to identify the status of the controls implementation for their respective systems. As a result, we identified [redacted] non-national security systems with an ATO in eMASS as of March 2024. Of those [redacted] systems, the DoD Components reported that

[23] (U) For FY 2024, we reviewed 37 metrics—20 Core and 17 FY 2024 Supplemental. Of the 37 assessed metrics, there were 35 metrics with 86 associated NIST information system controls in accordance with the IG FISMA reporting metrics guidance. The remaining two metrics—one Core and one FY 2024 Supplemental—did not have any associated NIST information system controls.

(U) The nine IG FISMA metrics were composed of seven Core and two FY 2024 Supplemental metrics.

~~(CUI)~~ they did not implement [redacted] of the [redacted] controls associated with 9 IG FISMA metrics (7 Core and 2 FY 2024 Supplemental) across 2 FISMA functions and 4 domains.[24] For example, DoD officials reported in eMASS that they did not consistently implement information system controls for their non-national security systems relating to the following metrics.

- ~~(CUI)~~ **Configuration Management** (*Metrics 20 and 21*): [redacted]
- ~~(CUI)~~ **Identity and Access Management** (*Metric 32*): [redacted]
- ~~(CUI)~~ **Data Protection and Privacy** (*Metrics 36 and 37*): [redacted]
- ~~(CUI)~~ **Contingency Planning** (*Metrics 61, 62, 63, and 64*): [redacted]

(U) Without the DoD Components consistently implementing the appropriate NIST controls and fully reporting the status in eMASS, or an equivalent system, for their non-national security systems, the DoD has no assurance that officials have the appropriate safeguards and procedures in place to effectively recover its data or operations from system disruptions or lower its risk of data breaches and unauthorized disclosures. Therefore, the DoD CIO should direct the DoD Components, including the Coast Guard, in coordination with their CISOs, CIOs, and AOs, to:

- (U) update eMASS, or an equivalent system, to ensure that it captures compliance information for all controls associated with IG FISMA reporting metrics for their non-national security systems;
- (U) develop and implement a process, such as periodic reviews of eMASS or an equivalent system, to ensure that officials implemented the necessary NIST information system controls and accurately reported the status for all non-national security systems; and
- (U) require officials to develop a plan of action and milestones for non-national security systems that have not implemented all IG FISMA reporting metrics-related controls or those systems with a low implementation percentage (for example, below 75 percent), and track the completion of the plans until such controls are implemented or have elevated to an acceptable level and are reported in eMASS, or an equivalent system.

[24] (U) We considered that the DoD Components generally implemented the NIST SP 800-53 information system control if officials reported in eMASS that the control was implement for 75 percent or more of the non-national security systems with an ATO.

(U) As previously reported, the DoD will not fully adopt NIST SP 800-53, Revision 5 controls for its non-national security systems until 2026, and thus we considered the associated NIST SP 800-53, Revision 4 controls, when applicable.

~~(CUI)~~ The Effectiveness of the DoD's Information Security Program [redacted] from FY 2021 Through FY 2024

~~(CUI)~~ The DoD continued to have [redacted] as defined by the annual IG FISMA reporting metrics guidance from FY 2021 through FY 2024, which fluctuated between the [redacted] maturity ratings. Although the DoD has taken steps to improve aspects of its information security program, [redacted]

(U) According to the IG FISMA reporting metrics guidance, IGs use a five-level IG FISMA maturity model when determining the agency's level of effectiveness of the information security program and associated system security controls. Within the context of the maturity model, the foundational levels require agencies to develop sound policies and procedures, while advanced levels capture the extent to which agencies institutionalize those policies and procedures. Operating at the Managed and Measurable (Level 4) or higher is considered an effective level of security. Additionally, IGs use a multistep process to determine the agency's overall effectiveness as it pertains to FISMA by using the:

- (U) outcome of the metrics to assign a domain maturity rating;
- (U) individual domain ratings to support the function ratings; and
- (U) corresponding function ratings to determine the agency's overall effectiveness.

~~(CUI)~~ For FY 2021 through FY 2024, we determined that the DoD [redacted] its information security program in accordance with IG FISMA reporting metrics guidance. Specifically, the DoD information security program's effectiveness fluctuated between the [redacted] maturity ratings, depending on the metrics reported and the scoring methodology used during the reporting period. See Figure 4 for the DoD's overall information security program effectiveness (FISMA) rating for FY 2021 through FY 2024 and how it relates to an effective level as defined by the annual IG FISMA reporting metrics guidance.

(U) Figure 4. FY 2021 Through FY 2024 DoD Overall FISMA Ratings

[redacted]

(U) Source: The DoD OIG.

~~(CUI)~~ Although the DoD's overall FISMA effectiveness rating is [redacted], the DoD's overall rating has remained relatively constant. [redacted]

~~(CUI)~~ *The DoD's NIST CSF Function Ratings Remained Relatively Constant* [redacted]

~~(CUI)~~ Although the DoD's NIST CSF function ratings remained relatively constant, its functional ratings [redacted] FY 2021 through FY 2024 as defined by the annual IG FISMA reporting metrics guidance. Specifically, [redacted] which were generally rated between the [redacted] maturity ratings; however, the [redacted] function has remained an area of strength and was consistently rated at an [redacted] which was at the [redacted] maturity rating. Figure 5 shows the DoD's maturity ratings for the five NIST CSF functions for FY 2021 through FY 2024.

(U) Figure 5. The DoD's Effectiveness by CSF Function Level

[redacted]

(U) Source: The DoD OIG.

(U) Identify Function

~~(CUI)~~ The DoD maturity level for the Identify function dropped from a [redacted] in FY 2021 to a [redacted] maturity rating from FY 2022 through FY 2024. This was generally due to the introduction of [redacted] and the DoD's continued challenges implementing [redacted] From FY 2022 to FY 2024, the DoD's maturity ratings for the Identify function consisted of [redacted] for the Risk Management domain and [redacted] for the SCRM domain. In addition, [redacted] some metrics within the Identify function addressed areas such as:

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

(U) Protect Function

~~(CUI)~~ The DoD maturity level for the Protect function has remained generally consistent at [redacted] from FY 2021 through FY 2024 and reached a [redacted] maturity level rating in FY 2022. This maturity level was generally due to the DoD demonstrating that it had established policies and procedures and implemented strong authentication to access all information systems and data encryption and to the specific metrics reported for each year.[25] However, the DoD had continued challenges implementing [redacted] From FY 2021 to FY 2024, the DoD's maturity ratings for the Protect function consisted of [redacted] maturity ratings for the Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains. In addition, [redacted] some of metrics within the Protect function addressed areas such as:

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

(U) Detect Function

~~(CUI)~~ The DoD maturity level for the Detect function has remained consistent at [redacted] for FY 2021 through FY 2024. Although the DoD continued to have some challenges regarding [redacted] it has operated at an [redacted] as defined by the IG FISMA reporting metrics guidance. This maturity level is generally due to the DoD demonstrating that it [redacted]

(U) Respond Function

~~(CUI)~~ The DoD maturity level for the Respond function has fluctuated between the [redacted] and [redacted] maturity ratings for FY 2021 through FY 2024. The assigned maturity levels were generally due to [redacted]

[25] ~~(CUI)~~ For example, the DoD information security maturity level for the Protect function increased to a [redacted] maturity rating in FY 2022 when the Identity and Access Management domain maturity rating increased from a [redacted] rating in FY 2021 to a [redacted] rating in FY 2022. When we only reviewed the three required core metrics for the Identity and Access Management domain, we determined that the DoD was operating at an effective security level in two of the three areas.

~~(CUI)~~ [redacted] From FY 2021 to FY 2024, the DoD's maturity ratings for the Respond function consisted of [redacted] and [redacted] maturity ratings for the Incident Response domain. In addition, [redacted] some of the metrics within the Respond function addressed areas such as:

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

(U) Recover Function

~~(CUI)~~ The DoD maturity level for the Recover function has remained consistent at [redacted] for FY 2021 through FY 2024. Although the DoD established and implemented some aspects of its contingency planning program, it [redacted] as defined by the IG FISMA reporting metrics guidance. From FY 2021 to FY 2024, the DoD's maturity ratings for the Recover function were at the [redacted] maturity rating for the Contingency Planning domain. [redacted]

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

~~(CUI)~~ Although the DoD began its [redacted] officials need [redacted] [redacted] as defined by IG FISMA reporting metric guidance. In addition, we have provided feedback on the DoD's effectiveness of its information security program through our annual FISMA reporting and previously issued FISMA-related reports. Implementing the recommendations made in those reports and the suggested corrective actions provided in our annual FISMA reporting should improve the DoD's overall effectiveness of its information security program.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the DoD Chief Information Officer direct DoD Components, including the Coast Guard, in coordination with the DoD Component Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to:

a. **(U) Identify all critical and non-critical software on the DoD Information Network that is subject to Office of Management and Budget-required self-attestation requirements.**

b. **(U) Obtain Office of Management and Budget-required self-attestations from software providers or implement an Office of Management and Budget-approved alternative solution for all identified third-party software on the DoD Information Network.**

c. **(U) Establish a plan of action and milestones to obtain all remaining Office of Management and Budget-required third-party provider self-attestations and request an extension from the Office of Management and Budget deadline.**

(U) DoD Chief Information Officer Comments

(U) Although the official Performing the Duties of the DoD CIO disagreed with Recommendation 1.a, they agreed with Recommendations 1.b and 1.c. The DoD CIO stated that a binary classification of software as “critical” or “non-critical” for public disclosure offers minimal benefit and may inadvertently increase the attack surface by highlighting the DoD’s critical assets to adversaries. They also stated that the OMB did not intend to grant extensions for collecting secure software development self-attestations as part of a May 2024 communication. However, the DoD CIO stated that the DoD remains committed to ensuring the secure development and deployment of third-party software on the DODIN, which is critical to the DoD’s cybersecurity posture.

(U) The DoD CIO also stated that the DoD attempted a few approaches to implement the OMB M-23-16 requirements but encountered potential contractual conflicts and cybersecurity policy limitations that would require the need for expanded criteria, independent verification, and continuous monitoring. The DoD CIO stated that these challenges led to the development of an emerging and more comprehensive SCRM program to strengthen software supply chain security that will address the limitations of relying solely on self-attestations from third-party software providers. This software SCRM program will be risk-based and incorporate expanded assessment criteria, independent verification mechanisms, and continuous monitoring throughout the software lifecycle to meet the intent of the OMB M-22-18 and OMB M-23-16 requirements. According to the DoD CIO, this risk-based approach will provide a more robust and adaptable framework for managing software supply chain risks for all DoD systems and applications. The DoD CIO also stated that they will continue to refine and implement the program to ensure a secure and resilient software ecosystem.

(U) Our Response

(U) Although the official Performing the Duties of the DoD CIO disagreed with Recommendation 1.a but agreed with Recommendations 1.b and 1.c, their comments addressed all specifics of the recommendations. Therefore, the recommendations are resolved but open. We will close the recommendations once the DoD CIO provides documentation demonstrating that the OMB has approved the DoD's alternative solution to strengthen its software supply chain security instead of obtaining the OMB-required self-attestations from software producers. The DoD CIO should also provide documentation demonstrating that they directed the DoD Components to implement the DoD's OMB-approved, alternative approach that meets the intent of the OMB M-22-18 and OMB M-23-16 requirements, including the: (1) identification of all applicable software on the DODIN; (2) procedures to ensure that third-party software providers followed NIST software development guidance for all applicable software on the DODIN; and (3) development of a plan of action and milestones to implement the DoD's OMB-approved, alternative approach.

d. **(U) Implement a process, such as periodic reviews of the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials are accurately reporting the system authorization status for non-national security systems in accordance with DoD guidance.**

(U) DoD Chief Information Officer Comments

(U) The official Performing the Duties of the DoD CIO agreed, stating that they intend to release a memorandum directing the DoD Components to review the proper guidelines for reporting the system authorization status and update the status for any miscategorized systems.

(U) Our Response

(U) Comments from the official Performing the Duties of the DoD CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the DoD CIO provides documentation demonstrating that they directed the DoD Components to implement a process, such as performing periodic reviews in eMASS or an equivalent system, to ensure that officials are accurately reporting the system ATO status for non-national security systems in accordance with DoD guidance.

e. **(U) Update the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that it captures compliance information for all controls associated with Inspector General Federal Information Security Modernization Act of 2014 reporting metrics for their non-national security systems.**

(U) DoD Chief Information Officer Comments

(U) The official Performing the Duties of the DoD CIO agreed with the recommendation, stating that they will update the Cyber Scorecard to include controls associated with the IG FISMA reporting metrics for non-national security systems.

(U) Our Response

(U) Comments from the official Performing the Duties of the DoD CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the DoD CIO provides documentation demonstrating that they updated the Cyber Scorecard to ensure that it captures the status of the controls associated with the IG FISMA reporting metrics for non-national security systems.

f. **(U) Develop and implement a process, such as periodic reviews of the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials implemented the necessary National Institute of Standards and Technology information system controls and accurately reported the status for all non-national security systems.**

(U) DoD Chief Information Officer Comments

(U) The official Performing the Duties of the DoD CIO agreed, stating that they will track the implementation of the necessary security controls in the Cyber Scorecard for the non-national security systems and add a statement to the Cyber Scorecard requiring that the DoD Components verify the accuracy of their submitted data.

(U) Our Response

(U) Comments from the official Performing the Duties of the DoD CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the DoD CIO provides documentation demonstrating that they updated the Cyber Scorecard to track the status of the NIST system controls for non-national security systems and added a statement to the Cyber Scorecard requiring that the DoD Components verify the accuracy of their submitted data.

g. **(U) Require officials to develop a plan of action and milestones for non-national security systems that have not implemented all Inspector General Federal Information Security Modernization Act of 2014 reporting metrics-related controls or those systems with a low implementation percentage (for example, below 75 percent), and track the completion of the plans until such controls are implemented or have elevated to an acceptable level and are reported in the Enterprise Mission Assurance Support Service, or an equivalent system.**

(U) DoD Chief Information Officer Comments

(U) The official Performing the Duties of the DoD CIO agreed, stating that they will add a metric to the Cyber Scorecard for tracking the status of non-compliant controls that are missing plan of action and milestones. The Scorecard will also track other controls associated with the IG FISMA reporting metrics that do not have a plan of action and milestones items.

(U) Our Response

(U) Comments from the official Performing the Duties of the DoD CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the DoD CIO provides documentation demonstrating that they added a metric to the Cyber Scorecard for tracking the status of non-compliant controls associated with the IG FISMA reporting metrics for non-national security systems, including whether the corresponding plan of action and milestones are reported in eMASS, or an equivalent system.

(U) Recommendation 2

(U) We recommend that the DoD Chief Information Officer direct the Army Chief Information Officer, in coordination with their Chief Information Security Officer and Authorizing Officials, to review the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials are correctly reporting the system authorization status for their non-national security systems and update the status for any miscategorized systems.

(U) Recommendation 3

(U) We recommend that the DoD Chief Information Officer direct the Navy Chief Information Officer, in coordination with their Chief Information Security Officer and Authorizing Officials, to review the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials are correctly reporting the system authorization status for their non-national security systems and update the status for any miscategorized systems.

(U) Recommendation 4

(U) We recommend that the DoD Chief Information Officer direct the Air Force Chief Information Officer, in coordination with their Chief Information Security Officer and Authorizing Officials, to review the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials are correctly reporting the system authorization status for their non-national security systems and update the status for any miscategorized systems.

(U) Recommendation 5

(U) We recommend that the DoD Chief Information Officer direct the Coast Guard Chief Information Officer, in coordination with their Chief Information Security Officer and Authorizing Officials, to review the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials are correctly reporting the system authorization status for their non-national security systems and update the status for any miscategorized systems.

(U) Recommendation 6

(U) We recommend that the DoD Chief Information Officer direct the Defense Security Cooperation Agency Chief Information Officer, in coordination with their Chief Information Security Officer and Authorizing Officials, to review the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials are correctly reporting the system authorization status for their non-national security systems and update the status for any miscategorized systems.

(U) DoD Chief Information Officer Comments

(U) The official Performing the Duties of the DoD CIO agreed with Recommendations 2, 3, 4, 5, and 6, stating that they will release a memorandum directing the DoD Components to review the proper guidelines for reporting the system authorization status and update the status for any miscategorized systems.

(U) Our Response

(U) Comments from the official Performing the Duties of the DoD CIO addressed all specifics of the recommendations; therefore, the recommendations are resolved but will remain open. We will close the recommendations once the DoD CIO provides documentation demonstrating that they directed the DoD Components to review the proper guidelines for reporting the system ATO status and update the status for any miscategorized systems in eMASS or their equivalent system.

(U) Appendix A

(U) Scope and Methodology

(U) We assessed the 37 metrics (20 core and 17 supplemental) of the DoD's information security program and practices as part of our FY 2024 annual independent review of the DoD's overall information security program and practices in accordance with the IG FISMA reporting metrics guidance. We submitted the results to the OMB, DHS, and DoD OCIO on July 30, 2024. We explained our rationale for each rating in the response to the summary metric questions for each domain and function and provided suggested actions the DoD could take to demonstrate that it is operating at the next maturity level.

(U) We are issuing this management advisory to report results from our FY 2024 FISMA review for selected metrics and to issue recommendations for corrective action. Of the 37 metrics that we assessed as part of our FY 2024 review, we are reporting on 12 metrics (10 Core and 2 FY 2024 Supplemental) that represent 7 of the 9 domains. We used a risk-based approach for selecting the metrics to report on in this management advisory to ensure that we covered most FISMA functions and domains. Table 2 shows the 12 metrics and the corresponding DoD FY 2024 maturity ratings that we are reporting on in this advisory. However, the results presented in this advisory do not fully represent all requirements for each metric or the DoD's overall rating as defined by IG FISMA reporting metric guidance.

(U) Table 2. IG FISMA Reporting Metrics Assessed

~~(CUI)~~ FISMA Function (Domain)	Metric No.	Metric Type	Metric Question	FY 2024 Assigned Maturity Rating
Identify (*Risk Management*)	3	Core	To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting?	[redacted]
Identify (*SCRM*)	14	Core	To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?	[redacted]
Protect (*Configuration Management*)	20	Core	To what extent does the organization use configuration settings/common secure configurations for its information systems?	[redacted]
Protect (*Configuration Management*)	21	Core	To what extent does the organization use flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities on all network addressable IP-assets?	[redacted] ~~(CUI)~~

(U) Table 2. IG FISMA Reporting Metrics Assessed (cont'd)

~~(CUI)~~ FISMA Function (Domain)	Metric No.	Metric Type	Metric Question	FY 2024 Assigned Maturity Rating
Protect (*Identity and Access Management*)	32	Core	To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed.	[redacted]
Protect (*Data Protection and Privacy*)	36	Core	To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle?	[redacted]
Protect (*Data Protection and Privacy*)	37	Core	To what extent has the organization implemented security controls (e.g., EDR) to prevent data exfiltration and enhance network defenses?	[redacted]
Detect *(ISCM)*	49	Core	How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls?	[redacted]
Recover (*Contingency Planning*)	61	Core	To what extent does the organization ensure that the results of BIAs are used to guide contingency planning efforts?	[redacted]
Recover (*Contingency Planning*)	62	FY 2024 Supplemental	To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans?	[redacted]
Recover (*Contingency Planning*)	63	Core	To what extent does the organization perform tests/exercises of its information system contingency planning processes?	[redacted]
Recover (*Contingency Planning*)	64	FY 2024 Supplemental	To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate?	[redacted] ~~(CUI)~~

(U) Source: The DoD OIG.

(U) To determine the findings and recommendations, we analyzed DoD information technology, cybersecurity, and privacy policies and procedures and corresponding controls from NIST SP 800-53. We reviewed key documents, such as monthly status reports that DoD officials used to track and monitor selected cybersecurity controls, plans for protecting

(U) sensitive information, other management reports supporting the DoD’s efforts to oversee the implementation of metric questions, and eMASS data. We also interviewed personnel from various DoD Components that were responsible for overseeing the implementation of cybersecurity and privacy-related policies and procedures, such as the:

- (U) DoD OCIO;
- (U) U.S. Cyber Command; and
- (U) Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency.

(U) Appendix B

(U) FY 2024 IG FISMA Reporting Metrics with Controls That Were Not Consistently Implemented DoD-Wide

~~(CUI)~~ Table 3 describes the 9 IG FISMA reporting metrics and the [redacted] associated NIST SP 800-53 information system controls that the DoD Components reported as not being implemented in eMASS for their non-national security systems with an ATO. We grouped the data by NIST information system control and, therefore, an IG FISMA Reporting Metric may be listed multiple times because some metrics have multiple associated controls. For example, Metric 20 is listed four times because it has [redacted] different NIST-associated controls [redacted]

(U) Table 3. IG FISMA Reporting Metrics Assessed

~~(CUI)~~ Function (*Domain*)	Metric No.	Metric Description	Metric Type	NIST SP 800-53, Rev 5 Control (Rev 4)	Control Description	No. of Non-Compliant Systems *(Percent)*
Protect (*Configuration Management*)	20	Security Configuration Settings	Core	[redacted]	[redacted]	[redacted]
Protect (*Configuration Management*)	20	Security Configuration Settings	Core	[redacted]	[redacted]	[redacted]
Protect (*Configuration Management*)	20	Security Configuration Settings	Core	[redacted]	[redacted]	[redacted]
Protect (*Configuration Management*)	21	Flaw Remediation	Core			
Protect (*Configuration Management*)	21	Flaw Remediation	Core	[redacted]	[redacted]	[redacted] ~~(CUI)~~
Protect (*Data Protection and Privacy*)	37	Data Exfiltration	Core			

(U) Table 3. IG FISMA Reporting Metrics Assessed (cont'd)

~~(CUI)~~

Function (*Domain*)	Metric No.	Metric Description	Metric Type	NIST SP 800-53, Rev 5 Control (Rev 4)	Control Description	No. of Non-Compliant Systems *(Percent)*
Protect (*Configuration Management*)	20	Security Configuration Settings	Core	[redacted]	[redacted]	[redacted]
Protect (*Configuration Management*)	21	Flaw Remediation	Core			
Protect (*Identity and Access Management*)	32	Least Privileged and Separation of Duties	Core	[redacted]	[redacted]	[redacted]
Protect (*Identity and Access Management*)	32	Least Privileged and Separation of Duties	Core	[redacted]	[redacted]	[redacted]
Protect (*Data Protection and Privacy*)	36	Privacy Controls	Core	[redacted]	[redacted]	[redacted]
Protect (*Data Protection and Privacy*)	36	Privacy Controls	Core	[redacted]	[redacted]	[redacted]
Recover (*Contingency Planning*)	61	Business Impact Analyses	Core	[redacted]	[redacted]	[redacted]
Recover (*Contingency Planning*)	61	Business Impact Analyses	Core	[redacted]	[redacted]	[redacted]
Recover (*Contingency Planning*)	62	Contingency Plan: Integration	Supplemental			
Recover (*Contingency Planning*)	63	Contingency Plan: Testing	Core	[redacted]	[redacted]	[redacted]

~~(CUI)~~

(U) Table 3. IG FISMA Reporting Metrics Assessed (cont'd)

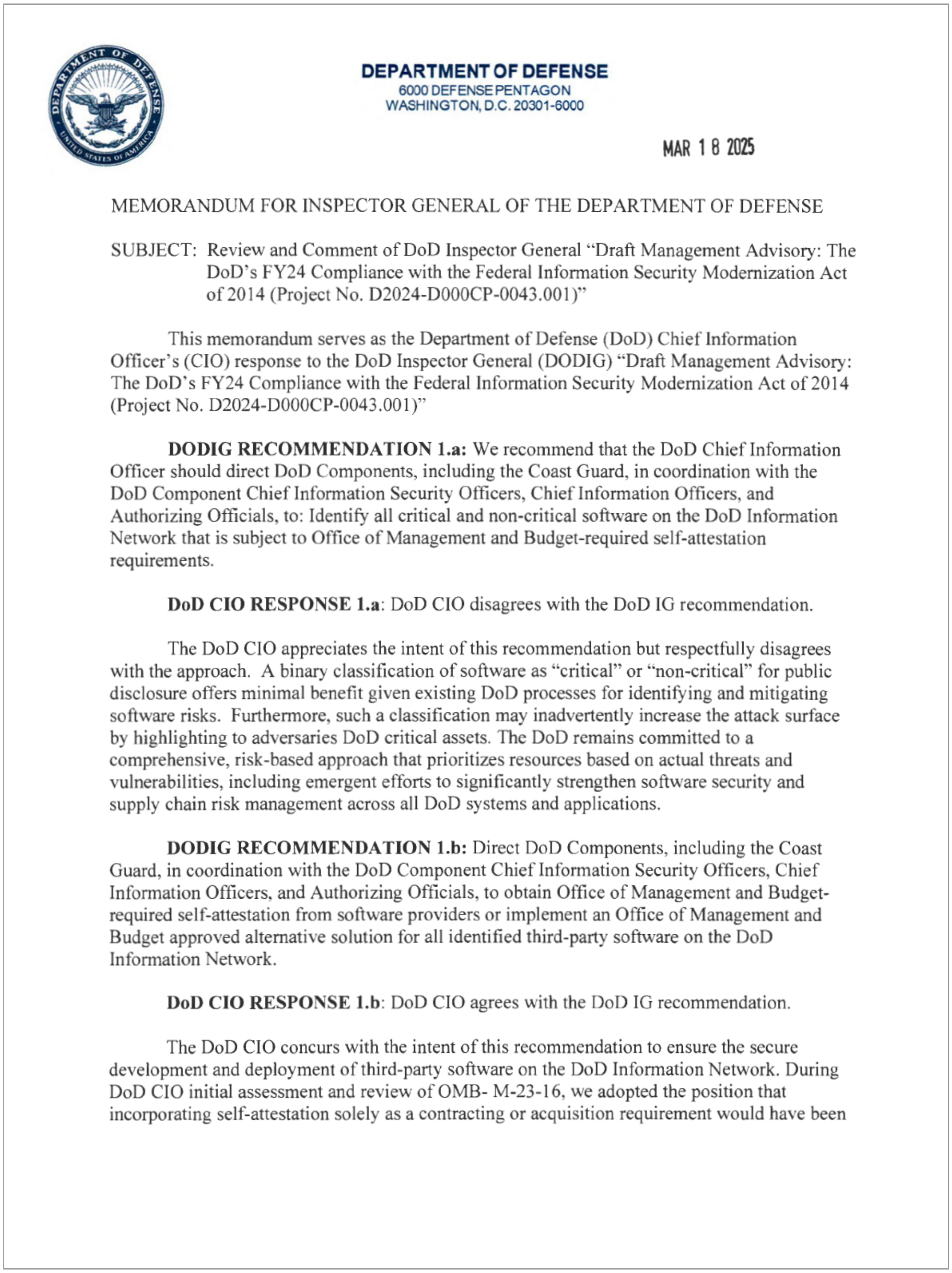
~~(CUI)~~ Function (*Domain*)	Metric No.	Metric Description	Metric Type	NIST SP 800-53, Rev 5 Control (Rev 4)	Control Description	No. of Non-Compliant Systems *(Percent)*
Recover (*Contingency Planning*)	63	Contingency Plan: Testing	Core	[redacted]	[redacted]	[redacted]
Recover (*Contingency Planning*)	64	Backup and Storage	Supplemental	[redacted]	[redacted]	[redacted]
Recover (*Contingency Planning*)	64	Backup and Storage	Supplemental	[redacted]	[redacted]	[redacted]
Recover (*Contingency Planning*)	64	Backup and Storage	Supplemental	[redacted]	[redacted]	[redacted]
Recover (*Contingency Planning*)	64	Backup and Storage	Supplemental	[redacted]	[redacted]	[redacted]
Recover (*Contingency Planning*)	64	Backup and Storage	Supplemental	[redacted]	[redacted]	[redacted] ~~(CUI)~~

* (U) For the contingency planning domain metrics (61, 62, 63, and 64), we only considered those systems compliant if the DoD Components reported in eMASS that they completed a BIA and implemented the associated NIST SP 800-53 controls.

(U) Source: The DoD OIG.

(U) Management Comments

(U) DoD Chief Information Officer



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

MAR 18 2025

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment of DoD Inspector General "Draft Management Advisory: The DoD's FY24 Compliance with the Federal Information Security Modernization Act of 2014 (Project No. D2024-D000CP-0043.001)"

This memorandum serves as the Department of Defense (DoD) Chief Information Officer's (CIO) response to the DoD Inspector General (DODIG) "Draft Management Advisory: The DoD's FY24 Compliance with the Federal Information Security Modernization Act of 2014 (Project No. D2024-D000CP-0043.001)"

DODIG RECOMMENDATION 1.a: We recommend that the DoD Chief Information Officer should direct DoD Components, including the Coast Guard, in coordination with the DoD Component Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to: Identify all critical and non-critical software on the DoD Information Network that is subject to Office of Management and Budget-required self-attestation requirements.

DoD CIO RESPONSE 1.a: DoD CIO disagrees with the DoD IG recommendation.

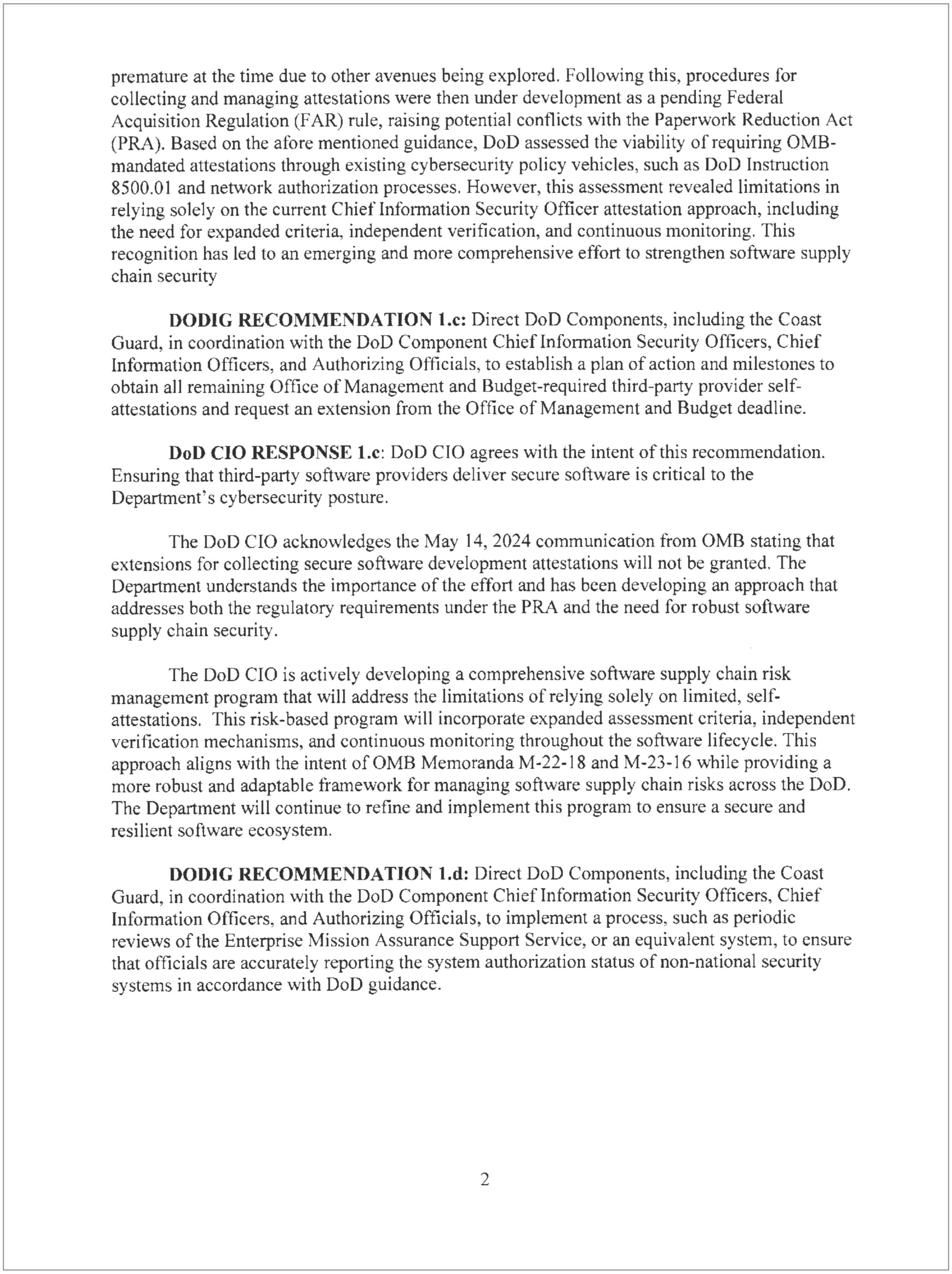
The DoD CIO appreciates the intent of this recommendation but respectfully disagrees with the approach. A binary classification of software as "critical" or "non-critical" for public disclosure offers minimal benefit given existing DoD processes for identifying and mitigating software risks. Furthermore, such a classification may inadvertently increase the attack surface by highlighting to adversaries DoD critical assets. The DoD remains committed to a comprehensive, risk-based approach that prioritizes resources based on actual threats and vulnerabilities, including emergent efforts to significantly strengthen software security and supply chain risk management across all DoD systems and applications.

DODIG RECOMMENDATION 1.b: Direct DoD Components, including the Coast Guard, in coordination with the DoD Component Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to obtain Office of Management and Budget-required self-attestation from software providers or implement an Office of Management and Budget approved alternative solution for all identified third-party software on the DoD Information Network.

DoD CIO RESPONSE 1.b: DoD CIO agrees with the DoD IG recommendation.

The DoD CIO concurs with the intent of this recommendation to ensure the secure development and deployment of third-party software on the DoD Information Network. During DoD CIO initial assessment and review of OMB- M-23-16, we adopted the position that incorporating self-attestation solely as a contracting or acquisition requirement would have been

(U) DoD Chief Information Officer (cont'd)



premature at the time due to other avenues being explored. Following this, procedures for collecting and managing attestations were then under development as a pending Federal Acquisition Regulation (FAR) rule, raising potential conflicts with the Paperwork Reduction Act (PRA). Based on the afore mentioned guidance, DoD assessed the viability of requiring OMB-mandated attestations through existing cybersecurity policy vehicles, such as DoD Instruction 8500.01 and network authorization processes. However, this assessment revealed limitations in relying solely on the current Chief Information Security Officer attestation approach, including the need for expanded criteria, independent verification, and continuous monitoring. This recognition has led to an emerging and more comprehensive effort to strengthen software supply chain security

DODIG RECOMMENDATION 1.c: Direct DoD Components, including the Coast Guard, in coordination with the DoD Component Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to establish a plan of action and milestones to obtain all remaining Office of Management and Budget-required third-party provider self-attestations and request an extension from the Office of Management and Budget deadline.

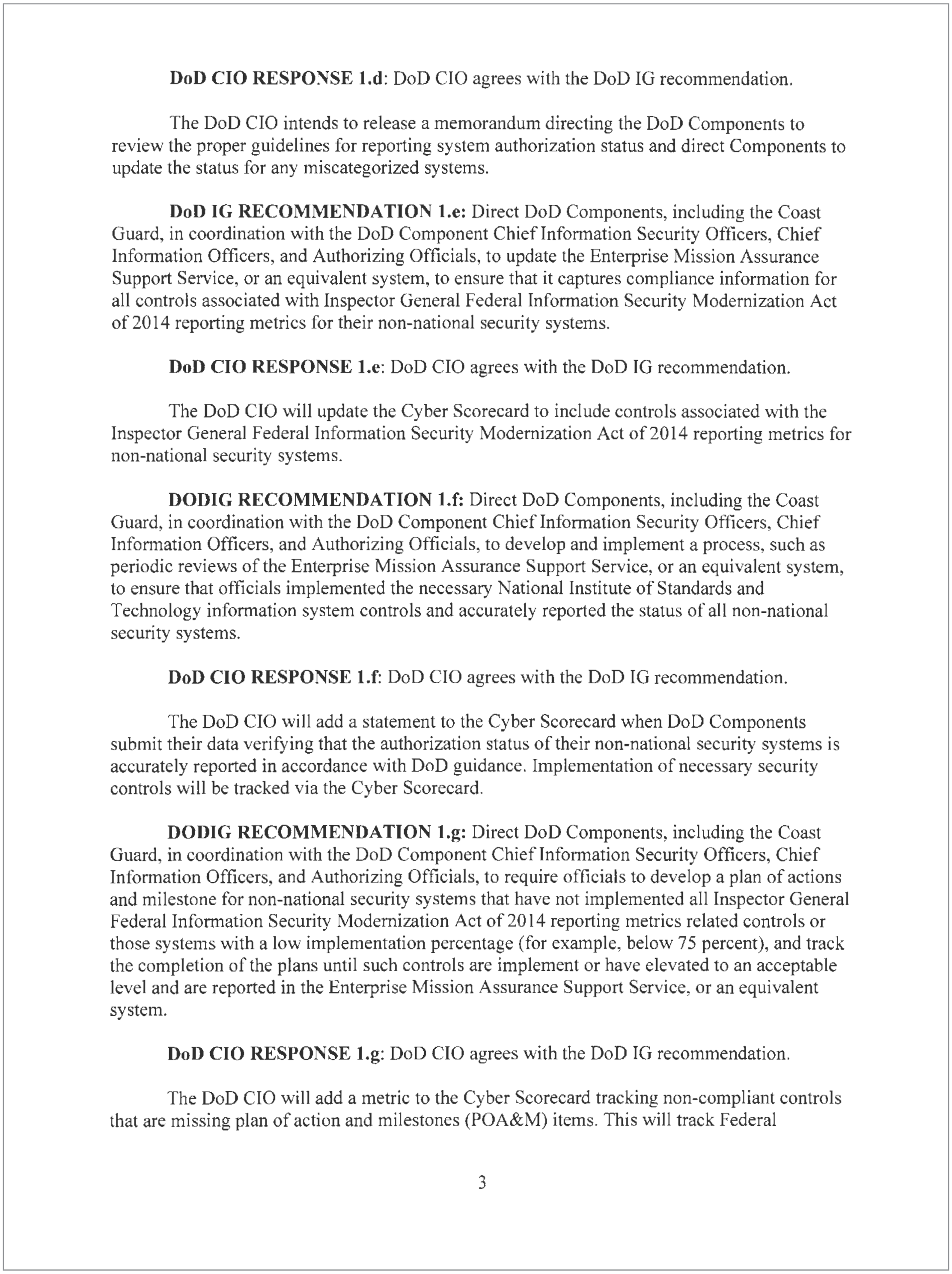
DoD CIO RESPONSE 1.c: DoD CIO agrees with the intent of this recommendation. Ensuring that third-party software providers deliver secure software is critical to the Department's cybersecurity posture.

The DoD CIO acknowledges the May 14, 2024 communication from OMB stating that extensions for collecting secure software development attestations will not be granted. The Department understands the importance of the effort and has been developing an approach that addresses both the regulatory requirements under the PRA and the need for robust software supply chain security.

The DoD CIO is actively developing a comprehensive software supply chain risk management program that will address the limitations of relying solely on limited, self-attestations. This risk-based program will incorporate expanded assessment criteria, independent verification mechanisms, and continuous monitoring throughout the software lifecycle. This approach aligns with the intent of OMB Memoranda M-22-18 and M-23-16 while providing a more robust and adaptable framework for managing software supply chain risks across the DoD. The Department will continue to refine and implement this program to ensure a secure and resilient software ecosystem.

DODIG RECOMMENDATION 1.d: Direct DoD Components, including the Coast Guard, in coordination with the DoD Component Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to implement a process, such as periodic reviews of the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials are accurately reporting the system authorization status of non-national security systems in accordance with DoD guidance.

(U) DoD Chief Information Officer (cont'd)



DoD CIO RESPONSE 1.d: DoD CIO agrees with the DoD IG recommendation.

The DoD CIO intends to release a memorandum directing the DoD Components to review the proper guidelines for reporting system authorization status and direct Components to update the status for any miscategorized systems.

DoD IG RECOMMENDATION 1.e: Direct DoD Components, including the Coast Guard, in coordination with the DoD Component Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to update the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that it captures compliance information for all controls associated with Inspector General Federal Information Security Modernization Act of 2014 reporting metrics for their non-national security systems.

DoD CIO RESPONSE 1.e: DoD CIO agrees with the DoD IG recommendation.

The DoD CIO will update the Cyber Scorecard to include controls associated with the Inspector General Federal Information Security Modernization Act of 2014 reporting metrics for non-national security systems.

DODIG RECOMMENDATION 1.f: Direct DoD Components, including the Coast Guard, in coordination with the DoD Component Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to develop and implement a process, such as periodic reviews of the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials implemented the necessary National Institute of Standards and Technology information system controls and accurately reported the status of all non-national security systems.

DoD CIO RESPONSE 1.f: DoD CIO agrees with the DoD IG recommendation.

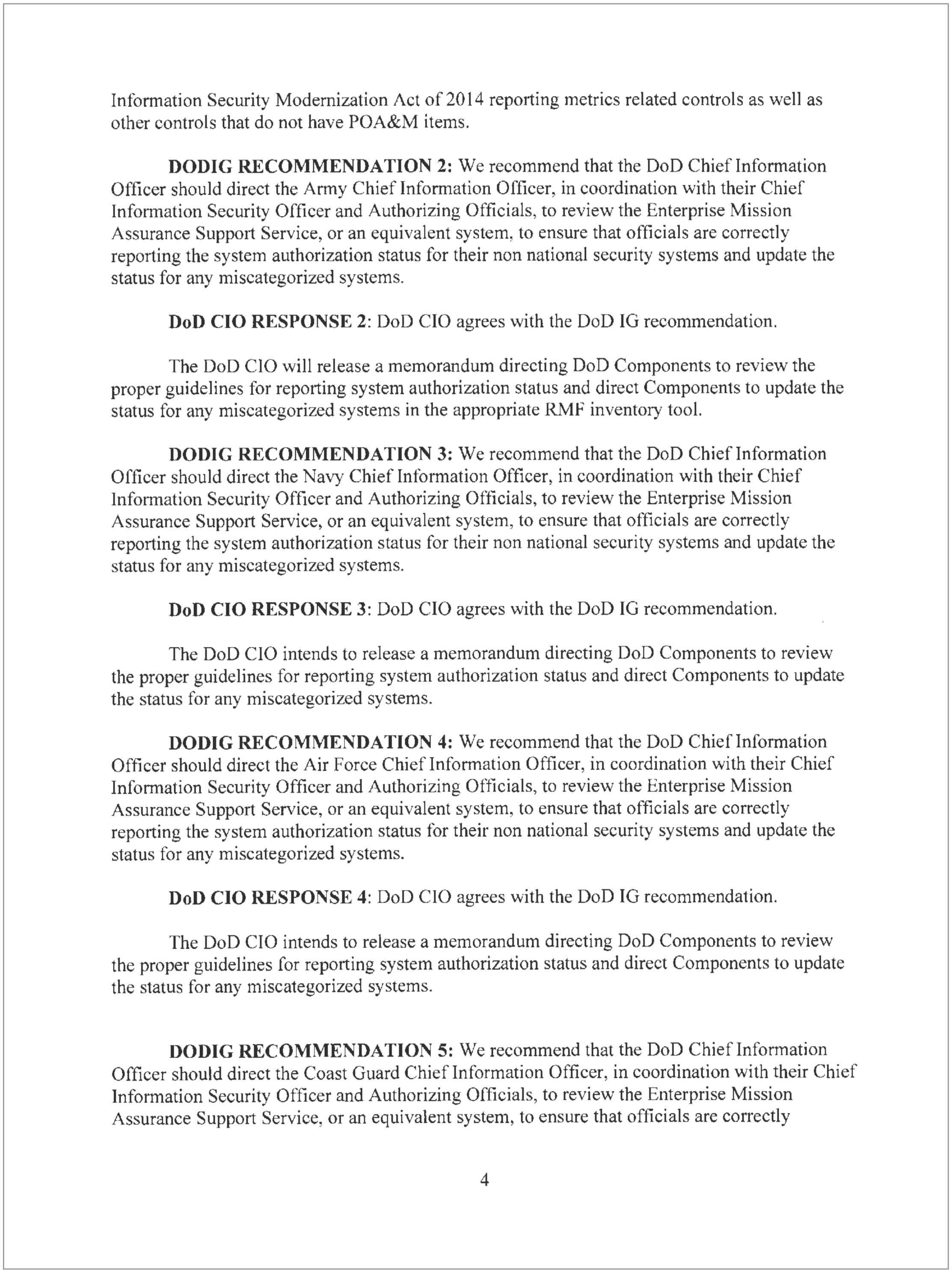
The DoD CIO will add a statement to the Cyber Scorecard when DoD Components submit their data verifying that the authorization status of their non-national security systems is accurately reported in accordance with DoD guidance. Implementation of necessary security controls will be tracked via the Cyber Scorecard.

DODIG RECOMMENDATION 1.g: Direct DoD Components, including the Coast Guard, in coordination with the DoD Component Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to require officials to develop a plan of actions and milestone for non-national security systems that have not implemented all Inspector General Federal Information Security Modernization Act of 2014 reporting metrics related controls or those systems with a low implementation percentage (for example, below 75 percent), and track the completion of the plans until such controls are implement or have elevated to an acceptable level and are reported in the Enterprise Mission Assurance Support Service, or an equivalent system.

DoD CIO RESPONSE 1.g: DoD CIO agrees with the DoD IG recommendation.

The DoD CIO will add a metric to the Cyber Scorecard tracking non-compliant controls that are missing plan of action and milestones (POA&M) items. This will track Federal

(U) DoD Chief Information Officer (cont'd)



Information Security Modernization Act of 2014 reporting metrics related controls as well as other controls that do not have POA&M items.

DODIG RECOMMENDATION 2: We recommend that the DoD Chief Information Officer should direct the Army Chief Information Officer, in coordination with their Chief Information Security Officer and Authorizing Officials, to review the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials are correctly reporting the system authorization status for their non national security systems and update the status for any miscategorized systems.

DoD CIO RESPONSE 2: DoD CIO agrees with the DoD IG recommendation.

The DoD CIO will release a memorandum directing DoD Components to review the proper guidelines for reporting system authorization status and direct Components to update the status for any miscategorized systems in the appropriate RMF inventory tool.

DODIG RECOMMENDATION 3: We recommend that the DoD Chief Information Officer should direct the Navy Chief Information Officer, in coordination with their Chief Information Security Officer and Authorizing Officials, to review the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials are correctly reporting the system authorization status for their non national security systems and update the status for any miscategorized systems.

DoD CIO RESPONSE 3: DoD CIO agrees with the DoD IG recommendation.

The DoD CIO intends to release a memorandum directing DoD Components to review the proper guidelines for reporting system authorization status and direct Components to update the status for any miscategorized systems.

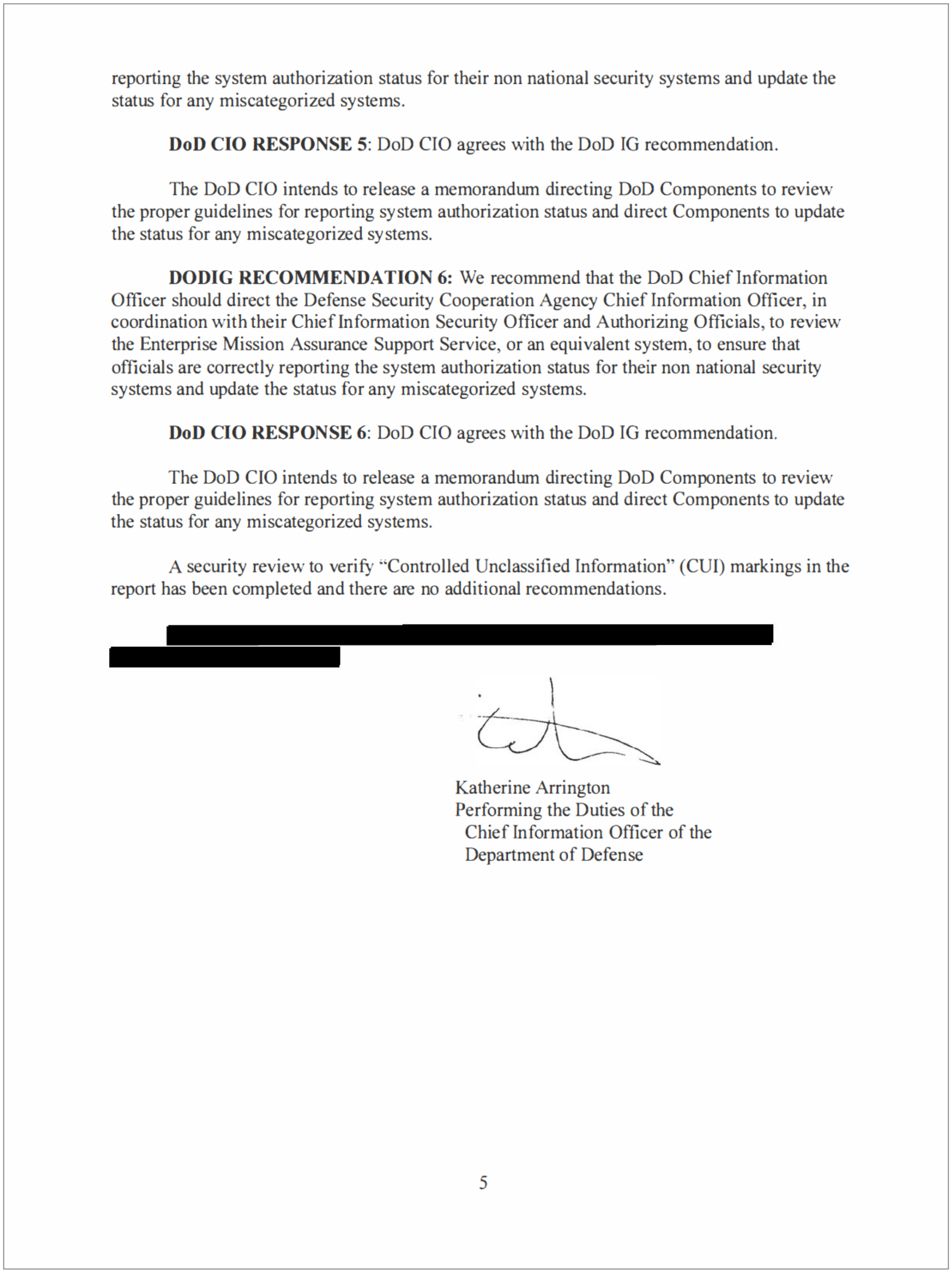
DODIG RECOMMENDATION 4: We recommend that the DoD Chief Information Officer should direct the Air Force Chief Information Officer, in coordination with their Chief Information Security Officer and Authorizing Officials, to review the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials are correctly reporting the system authorization status for their non national security systems and update the status for any miscategorized systems.

DoD CIO RESPONSE 4: DoD CIO agrees with the DoD IG recommendation.

The DoD CIO intends to release a memorandum directing DoD Components to review the proper guidelines for reporting system authorization status and direct Components to update the status for any miscategorized systems.

DODIG RECOMMENDATION 5: We recommend that the DoD Chief Information Officer should direct the Coast Guard Chief Information Officer, in coordination with their Chief Information Security Officer and Authorizing Officials, to review the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials are correctly

(U) DoD Chief Information Officer (cont'd)



reporting the system authorization status for their non national security systems and update the status for any miscategorized systems.

DoD CIO RESPONSE 5: DoD CIO agrees with the DoD IG recommendation.

The DoD CIO intends to release a memorandum directing DoD Components to review the proper guidelines for reporting system authorization status and direct Components to update the status for any miscategorized systems.

DODIG RECOMMENDATION 6: We recommend that the DoD Chief Information Officer should direct the Defense Security Cooperation Agency Chief Information Officer, in coordination with their Chief Information Security Officer and Authorizing Officials, to review the Enterprise Mission Assurance Support Service, or an equivalent system, to ensure that officials are correctly reporting the system authorization status for their non national security systems and update the status for any miscategorized systems.

DoD CIO RESPONSE 6: DoD CIO agrees with the DoD IG recommendation.

The DoD CIO intends to release a memorandum directing DoD Components to review the proper guidelines for reporting system authorization status and direct Components to update the status for any miscategorized systems.

A security review to verify "Controlled Unclassified Information" (CUI) markings in the report has been completed and there are no additional recommendations.

[redacted]

Katherine Arrington
Performing the Duties of the
Chief Information Officer of the
Department of Defense

Whistleblower Protection

U.S. Department of Defense

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:

Legislative Affairs Division
703.604.8324

Public Affairs Division
public.affairs@dodig.mil; 703.604.8324

www.dodig.mil

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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