

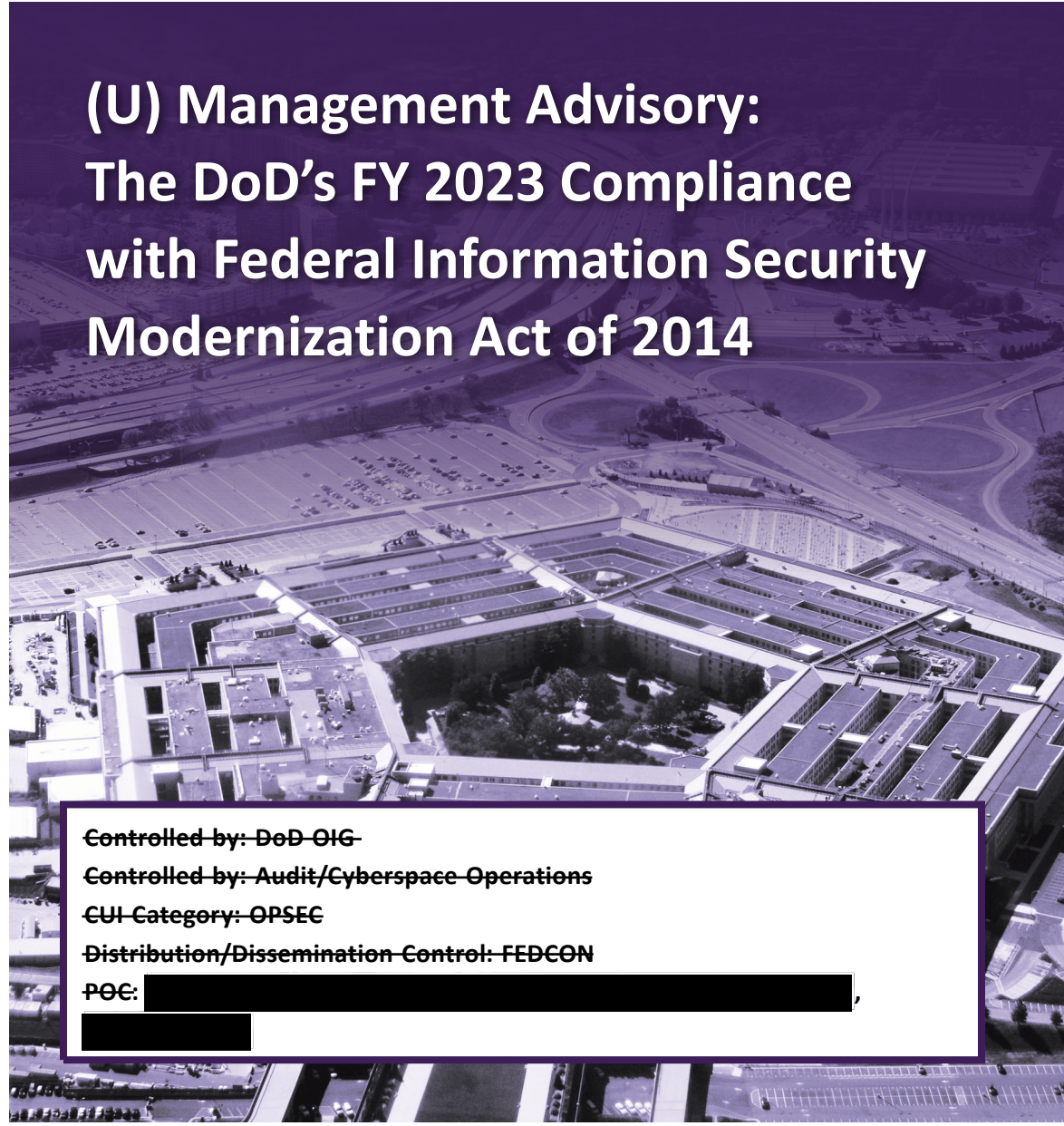


CUI

# INSPECTOR GENERAL

*U.S. Department of Defense*

MAY 21, 2024



## (U) Management Advisory: The DoD's FY 2023 Compliance with 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],  
[REDACTED]

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

CUI







CUI

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

May 21, 2024

MEMORANDUM FOR CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE

SUBJECT: (U) Management Advisory: The DoD's FY 2023 Compliance with Federal Information Security Modernization Act of 2014 (Report No. DODIG-2024-084)

(U) This management advisory provides the results of the DoD Office of Inspector General's review of the DoD's compliance with Federal Information Security Modernization Act of 2014 (FISMA). We identified the findings during our FY 2023 review of the DoD's compliance with FISMA, which was announced on November 14, 2022 (Project No. D2023-D000CP-0026.000). We conducted work on this project from November 2022 to December 2023 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. We consider one recommendation closed because management took action sufficient to address the recommendation, three recommendations unresolved because the DoD CIO did not fully address the recommendations presented in the report, and eight recommendations resolved but open. We will track the unresolved recommendations until management has agreed to take actions that we determine to be sufficient to meet the intent of the recommendations and management officials submit adequate documentation showing that all agreed-upon actions are completed. We will close the resolved 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. For the unresolved recommendations, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations. Send your response as a PDF file to [audcso@dodig.mil](mailto:audcso@dodig.mil). For the resolved recommendations, please provide us documentation within 90 days showing you have completed the agreed-upon actions. Send your response as a PDF file to either [followup@dodig.mil](mailto:followup@dodig.mil) if unclassified or [rfunet@dodig.smil.mil](mailto:rfunet@dodig.smil.mil) if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

CUI

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

FOR THE INSPECTOR GENERAL:

A handwritten signature in black ink, appearing to read "Carol N. Gorman". The signature is fluid and cursive, with a horizontal line extending from the end.

Carol N. Gorman  
Assistant Inspector General for Audit  
Cyberspace Operations



## (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 Office of Management and Budget’s (OMB) 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. FISMA requires that senior agency officials 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, Department of Homeland Security, and risk-based standards and guidelines published by the National Institute of Standards and Technology (NIST).<sup>1</sup>

*(U) FISMA requires that senior agency officials provide security for the information and information systems that support the operations and assets under their control.*

(U) FISMA also requires that Federal agencies 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 OMB and Department of Homeland Security. 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.<sup>2</sup> The OMB, Department of Homeland Security, and Council of the Inspectors General on Integrity and Efficiency develop the IG FISMA reporting metrics, in consultation with the Federal Chief Information Officer (CIO) Council.

<sup>1</sup> (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.

<sup>2</sup> (U) For FY 2023 FISMA guidance, the OMB issued Memorandum M-23-03, “Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements,” on December 2, 2022.

## (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—Identify, Protect, Detect, Respond, and Recover.<sup>3</sup> The NIST Cybersecurity Framework 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.<sup>4</sup> Table 1 lists the nine FISMA domains by NIST 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 before they receive access to organizational information technology resources, including specialized training for individuals requiring privileged access.

(U)

<sup>3</sup> (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.

<sup>4</sup> (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
Detect	Information Security Continuous Monitoring	Information security continuous monitoring is the process for maintaining ongoing awareness of information security, vulnerabilities, and threats to support operational risk management decisions.
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 also use NIST Special Publication (SP) 800-53, Revision 5 controls, Executive Orders, OMB guidance, and other Federal information security guidance as criteria for assessing the effectiveness of an agency's information security program and practices.<sup>5</sup>

## (U) DoD Roles and Responsibilities for Information Security

(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.<sup>6</sup> 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 (AO).** AOs make authorization decisions for information technology systems, which is also known as the authorization to operate (ATO) process.<sup>7</sup> 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) **CIO.** 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 Chief Information Security Officer (CISO).<sup>8</sup> The DoD Component CIOs, on behalf of the respective DoD Component heads, develop, implement, maintain, and enforce a DoD Component cybersecurity program and appoint DoD Component CISOs to direct and coordinate the DoD Component cybersecurity program.

<sup>5</sup> (U) NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5, updated December 2020.

<sup>6</sup> (U) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, Incorporating Change 1, Effective October 7, 2019.

<sup>7</sup> (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.

<sup>8</sup> (U) DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022, refers to the Senior Information Security Officer as the CISO. Therefore, we will use the term CISO for this management advisory.



(U) **CISO.** The DoD CISO, on behalf of 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.

(U) **Director for Defense Privacy and Civil Liberties.** The Director for the Defense Privacy and Civil Liberties Directorate oversees and implements the DoD Privacy and Civil Liberties Programs and ensures that guidance, assistance, and subject matter support are provided to DoD Components in the implementation and execution of DoD Privacy and Civil Liberties Programs.

(U) **Senior Agency Official for Privacy.** The DoD Senior Agency Official for Privacy oversees, coordinates, and facilitates the DoD's privacy and civil liberties compliance efforts and manages privacy risks associated with personally identifiable information (PII) specific to DoD programs and information systems.<sup>9</sup> The Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency is the DoD Senior Agency Official for Privacy.

## (U) DoD Information Security Program and Practices

(U) Although the DoD generally had information security-related policies and procedures in place for the six IG FISMA metrics that we are reporting on (see the Appendix for a list of the six metrics), DoD officials did not consistently comply with NIST or DoD guidance when implementing those policies and procedures. Specifically, DoD officials did not:

- (U) issue a DoD-wide supply chain risk management (SCRM) strategy or implementing guidance that addressed all SCRM-related NIST requirements;
- (U) consistently conduct a privacy impact assessment (PIA) to identify and mitigate the privacy-related risks for information systems with PII as required by NIST guidance or report the completion of PIAs as required by DoD guidance;
- (U) always develop a business impact analysis (BIA) for information systems as required by NIST guidance or report the completion of the BIAs as required by DoD guidance; or

*(U) Although the DoD generally had information security-related policies and procedures in place for the six IG FISMA metrics that we are reporting on DoD officials did not consistently comply with NIST or DoD guidance when implementing those policies and procedures.*

<sup>9</sup> (U) PII is information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, or biometric records, and any other personal information that is linked or linkable to a specified individual.

- (U) always conduct information system contingency plan testing as required by NIST and DoD guidance or report when the plan was tested as required by DoD guidance.

(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.

(U) Additionally, we identified that the DoD CIO has not fully implemented the DoD's cybersecurity policies and procedures to reflect updates outlined in NIST SP 800-53, Revision 5. The DoD Office of the Chief Information Officer (OCIO) plans to require that the DoD Components implement the updated NIST requirements in a phased approach as part of the systems' ATO process. As a result, the DoD will not fully implement the updated NIST requirements for all systems until 2026, which is 6 years after NIST issued the revision. Until the DoD revises its cybersecurity policies and procedures and fully implements the updated NIST guidance, DoD officials are limited in their ability to operate at an effective level of security as defined by IG FISMA reporting metric guidance.

*(U) DoD CIO has not fully implemented the DoD's cybersecurity policies and procedures to reflect updates outlined in NIST SP 800-53, Revision 5.*

## **(U) SCRM Domain**

### **(U) DoD Lacks an Overall SCRM-Related Strategy and Guidance**

(U) The DoD CIO did not issue a DoD-wide SCRM strategy or implementing guidance that addressed all SCRM-related NIST requirements. According to NIST, SCRM includes the management of security and privacy risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services.

(U) NIST SP 800-53 requires the development and implementation of an organizational-wide SCRM strategy for managing supply chain risks, which should be implemented consistently across the organization and continuously updated to address organizational changes. A SCRM strategy should include the organization-level risk appetite and tolerance, risk mitigation strategies and controls, a process for consistently evaluating and monitoring risk, approaches for implementing and communicating the strategy, and the associated roles and responsibilities. The SCRM-related policies and procedures should implement the strategy, define baseline controls, and establish roles and responsibilities. In addition, NIST SP 800-161 provides guidance for Federal agencies

(U) to use to identify, assess, and mitigate cybersecurity risks throughout the supply chain at all levels of an organization, including the development of SCRM strategy implementation plans, policies and procedures, and risk assessments for using external provider products and services.<sup>10</sup>

(U) Although the DoD has SCRM-related policies and procedures, the policies and procedures do not constitute a DoD-wide SCRM strategy to manage supply chain risks consistently throughout the product or service's life cycle or address all of the elements required by NIST SP 800-53. The DoD issued SCRM-related guidance, such as DoD Instruction 4140.67, DoD Instruction 5000.83, DoD Instruction 5000.90, and DoD Instruction 5200.44, that collectively require DoD Components to minimize the supply chain risks that impact the DoD's mission.<sup>11</sup> For example, DoD Instruction 5000.83 assigns responsibilities and provides

*(U) Although the DoD has SCRM-related policies and procedures, the policies and procedures do not constitute a DoD-wide SCRM strategy to manage supply chain risks consistently throughout the product or service's life cycle.*

procedures for managing system security and cybersecurity technical risks from supply chain exploitation and reverse engineering. In addition, the DoD OCIO developed a draft Information Communications Technology strategy that outlines a risk-based approach to ensure that cyber risks are visible at all levels of procurement. However, the DoD Instructions and draft Information

Communications Technology strategy do not include an organizational-wide SCRM terminology (taxonomy), baseline controls, governance structure, or an oversight process to ensure that DoD Components are consistently assessing, responding to, and monitoring supply chain risks throughout the life cycle for products or services. The DoD SCRM-related guidance also does not require the DoD Components to develop and issue implementing guidance that addresses Component-specific risk tolerances and activities for SCRM.

(U) Additionally, the DoD did not establish an organizational-wide risk appetite and tolerance or processes for monitoring risk throughout the life cycle for products and services from external providers. DoD Instruction 5000.90 states that program managers should have situational awareness of the supply chain risks and vulnerabilities throughout the program's life cycle. DoD Instruction 4140.67 assigns responsibilities for the prevention, detection, remediation, investigation, and restitution to defend against counterfeit materiel that poses a threat to personnel safety and mission assurance. In addition, DoD OCIO officials stated that the DoD uses various tools on a limited scale to evaluate cyber supply chain risks and that

<sup>10</sup> (U) NIST SP 800-161, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," published in May 2022. An external provider provides a product or service through a contract, agreement, or other business arrangement to an organization that has no direct control over the implementation of required security and privacy controls or the assessment of control effectiveness.

<sup>11</sup> (U) DoD Instruction 4140.67, "DoD Counterfeit Prevention Policy," April 26, 2013, Incorporating Change 3, Effective March 6, 2020.  
 (U) DoD Instruction 5000.83, "Technology and Program Protection to Maintain Technological Advantage," July 20, 2020, Incorporating Change 1, Effective May 21, 2021.  
 (U) DoD Instruction 5000.90, "Cybersecurity for Acquisition Decision Authorities and Program Managers," December 31, 2020.  
 (U) DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012, Incorporating Change 3, Effective October 15, 2018.



(U) they planned to issue guidance that addresses the DoD's requirements for maintaining awareness of its upstream suppliers (external providers). However, the DoD Instructions that address SCRM do not fully establish an organizational-wide process for DoD Components to consistently manage supply chain risks from external providers. DoD OCIO officials explained that they are updating SCRM-related guidance, such as DoD Instruction 5200.44, but the Instruction, DoD-wide SCRM strategy, and the SCRM-related procedures had not been issued as of November 2023.

(U) The lack of a DoD-wide SCRM strategy and implementing guidance—such as policies, procedures, and tools for managing cybersecurity and supply chain risks associated with using external providers, limits the DoD's ability to consistently and effectively manage evolving cybersecurity-related supply chain risks. Therefore, the DoD CIO should develop, in coordination with the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment, a DoD-wide SCRM strategy as required by NIST guidance. Once the DoD-wide SCRM strategy is issued, the DoD CIO should develop, in coordination with the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment, policies and procedures implementing the strategy as required by NIST guidance, including organizational-wide tools and techniques that allow DoD Components to consistently and effectively manage risks associated with using external providers.

*(U) The lack of a DoD-wide SCRM strategy and implementing guidance limits the DoD's ability to consistently and effectively manage evolving cybersecurity-related supply chain risks.*

## **(U) Data Protection and Privacy Domain**

### **(U) DoD Officials Did Not Conduct PIAs for Information Systems**

(U) Although the DoD had privacy-related policies and procedures implementing a DoD-wide privacy program, DoD Component officials did not consistently conduct PIAs to identify and mitigate the privacy-related risks for information systems with PII as required by NIST guidance or report the completion of PIAs as required by DoD guidance.<sup>12</sup> A PIA is an analysis of how PII is collected, used, shared, and maintained to: (1) ensure that it conforms to applicable legal and regulatory privacy-related requirements, (2) determine the risks and effects of having PII in an information system, and (3) evaluate protections and alternate processes for handling information to mitigate potential privacy-related concerns.

<sup>12</sup> (U) An information system is considered to have PII if it collects, uses, maintains, shares, or disposes of any PII-related information.

(U) NIST SP 800-53 requires that organizations conduct PIAs for systems, programs, or other activities before developing or procuring information technology that processes PII or initiating a new collection of PII that will be processed using information technology. DoD Instruction 5400.16 incorporates the NIST SP 800-53 privacy requirements for handling PII.<sup>13</sup> For example, DoD Instruction 5400.16 requires DoD Components to review their information systems to determine whether they process PII and, if an information system processes PII, the DoD Components should complete a PIA. DoD Instruction 5400.16 also requires DoD Components to synchronize the review and update of PIA in conjunction with the information system's ATO. 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 the Enterprise Mission Assurance Support Service (eMASS) or an equivalent system.<sup>14</sup>

~~(CUI)~~ To determine whether the DoD Components were completing the required PIAs and reporting the completion of the PIAs in eMASS for information systems that had PII, we reviewed eMASS data to identify whether officials indicated that the system had PII and a completed PIA.<sup>15</sup> As a result, we identified [REDACTED] non-national security systems in eMASS as of May 2023.<sup>16</sup> Of the [REDACTED] systems, DoD Components indicated that [REDACTED] systems had PII. Of the [REDACTED] systems with PII, the DoD Components indicated that they did not complete or report that they completed a PIA for [REDACTED] systems [REDACTED] as required by NIST SP 800-53 and DoD Instruction 5400.16.

(U) Additionally, DoD OCIO officials issued conflicting guidance as to when DoD Components should complete PIAs for information systems. According to the DoD Risk Management Framework (RMF) Knowledge Service, DoD Components should complete PIAs, in coordination with an organizational privacy subject matter expert, for all information systems as part of the ATO process regardless of whether the information system processes PII.<sup>17</sup>

<sup>13</sup> (U) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, Incorporating Change 1, Effective August 11, 2017.

<sup>14</sup> (U) eMASS is a tool that captures key information system documentation from the DoD Risk Management Framework (RMF) process, such as system security plans, security control test results, plans of action and milestones, and authorization decisions.

<sup>15</sup> ~~(CUI)~~ We reviewed eMASS to determine whether DoD officials indicated that they completed the required PIAs for the [REDACTED] systems that had an ATO and did not obtain the PIAs or validate the information with the DoD Components.

<sup>16</sup> (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 considered any system that is not categorized as a national security system. (U) We reviewed non-national security systems that had an ATO from eMASS because NIST SP 800-53 applies only to non-national security systems, and eMASS is the primary tool used by the DoD Components, which is referenced in DoD RMF guidance.

<sup>17</sup> (U) The RMF Knowledge Service is a web-based resource serving as the authoritative source for standardized implementation of the RMF and the repository for DoD RMF policies and procedures.

(~~CUI~~) To determine whether the DoD Components were completing PIAs and reporting the completion of the PIAs in eMASS for all information systems regardless of whether the system had PII, we reviewed eMASS data to identify whether officials indicated that they completed a PIA for the system. Of the [REDACTED] systems, the DoD Components indicated that they did not prepare or report that they completed a PIA for [REDACTED] systems [REDACTED] as required by the DoD RMF Knowledge Service guidance.

(U) Without establishing clear guidance for when DoD Components should complete PIAs or for consistently completing PIAs to manage its privacy-related risks, the DoD limited its ability to ensure that officials applied the proper controls to safeguard PII and prevent unauthorized access or disclosure

*(U) Without establishing clear guidance for when DoD Components should complete PIAs, the DoD limited its ability to ensure that officials applied the proper controls to safeguard PII and prevent unauthorized access or disclosure of PII.*

of PII. Therefore, the DoD CIO should determine when DoD Components should complete a PIA for information systems and ensure that all DoD guidance, including DoD Instruction 5400.16 and the DoD RMF Knowledge Service, aligns with that determination. The DoD CIO should direct DoD Components, in coordination with the CISOs, CIOs, and AOs, to require that officials conduct PIAs for all non-national security systems and update eMASS, or its equivalent system, as required by DoD guidance. The DoD CIO should also implement a process, in coordination with the DoD Component CISOs, CIOs, and AOs, such as periodic eMASS reviews, to ensure that officials complete PIAs for all non-national security systems and update eMASS, or an equivalent system, as required by DoD guidance.

## (U) Contingency Planning Domain

### **(U) DoD Officials Did Not Develop BIAs for Information Systems**

(U) DoD Components did not always develop BIAs for information systems as required by NIST guidance or report the completion of the BIAs as required by DoD guidance. The BIA identifies an information system's components and supported critical mission processes to assist in determining the consequences of a system disruption due to an emergency, system failure, or a disaster. Information system owners use the results of BIAs to develop contingency plan requirements and priorities to mitigate the identified consequences.

(U) NIST SP 800-53 requires that organizations develop BIAs to determine contingency planning requirements and priorities. DoD Instruction 8500.01 requires DoD Components to develop contingency plans using guidance found in NIST SP 800-34, which requires information system owners to develop a BIA as the second step of the information system contingency planning process to determine contingency planning requirements and priorities.<sup>18</sup> DoD RMF guidance requires the DoD Components to develop BIAs as part of the ATO process and document whether they completed a BIA in eMASS or an equivalent system.

<sup>18</sup> (U) NIST SP 800-34, "Contingency Planning Guide for Federal Information Systems," Published May 2010.



(CUI) To determine whether the DoD Components developed the required BIAs and reported the completion of the BIAs in eMASS, we reviewed eMASS data to identify whether officials indicated that they completed a BIA for the system.<sup>19</sup> Of the [REDACTED] systems, the DoD Components indicated that they did not complete or report that they completed a BIA for [REDACTED] systems [REDACTED] as required by NIST SP 800-53 and DoD Instruction 8500.01.

*(U) Without a BIA to guide their information system contingency planning efforts, DoD Components do not have assurance that officials correctly identified the resource requirements and recovery priorities to effectively recover their information systems after a disruption.*

(U) Without a BIA to guide their information system contingency planning efforts, DoD Components do not have assurance that officials correctly identified the resource requirements and recovery priorities to effectively recover their information systems after a disruption. Therefore, the DoD CIO

should direct DoD Components, in coordination with the CISOs, CIOs, and AOs, to conduct BIAs for all non-national security systems and update eMASS, or an equivalent system, as required by DoD guidance. The DoD CIO should also implement a process, in coordination with the DoD Component CISOs, CIOs, and AOs, such as periodic eMASS reviews, to ensure that DoD officials complete BIAs for all non-national security systems and update eMASS, or its equivalent system, as required by DoD guidance.

### ***(U) DoD Officials Did Not Test Information System Contingency Plans***

(U) DoD Components did not always conduct information system contingency plan testing as required by NIST and DoD guidance or report when the plan was tested as required by DoD guidance. An information system contingency plan contains the policies and procedures designed to maintain or restore the system, operations, and data after a system disruption due to an emergency, system failure, or a disaster.

(U) NIST SP 800-53 requires that organizations test or exercise information system contingency plans to determine their effectiveness and to ensure that personnel are properly trained to execute the plan. Testing may include checklists, walkthroughs or tabletop exercises, or simulations. In addition, DoD Directive 3020.26 requires that DoD Components annually test the information systems contingency plans to evaluate and validate the plan's readiness.<sup>20</sup> DoD RMF guidance also requires that the DoD Components document the test results in eMASS or an equivalent system.

*(U) Organizations test or exercise information system contingency plans to determine their effectiveness and to ensure that personnel are properly trained to execute the plan.*

<sup>19</sup> (CUI) We reviewed eMASS to determine whether DoD officials indicated that they completed the required BIAs for the [REDACTED] systems that had an ATO and did not obtain the BIAs or validate the information with the DoD Components.

<sup>20</sup> (U) DoD Directive 3020.26, "DoD Continuity Policy," February 14, 2018.

(CUI) To determine whether DoD Components conducted information system contingency plan testing and reported the plan test date in eMASS, we reviewed eMASS data to identify whether officials indicated that they had a contingency plan and a plan test date for the system.<sup>21</sup> Of the [REDACTED] systems, DoD Components indicated that [REDACTED] systems had an information system contingency plan. Of the [REDACTED] systems with a plan, DoD Components officials indicated that they did not test the plan for [REDACTED] systems [REDACTED]. Of the [REDACTED] systems with a tested plan, DoD Components officials did not indicate that they annually tested the plan for [REDACTED] systems [REDACTED] in accordance with DoD guidance.

(U) If the DoD Components do not properly perform tests of their information system contingency plans or conduct tests annually, then DoD officials may not effectively restore information systems or recover data in a timely manner to minimize the negative impact to critical missions after a system disruption. Therefore, the DoD CIO should direct the DoD Components, in coordination with the CISOs, CIOs, and AOs, to conduct information system contingency plan testing, including annual testing for all non-national security systems and update eMASS, or its equivalent system, as required by DoD guidance. The DoD CIO should implement a process, in coordination with the CISOs, CIOs, and AOs, such as periodic eMASS reviews, to ensure that DoD officials are annually testing contingency plans for all non-national security systems and eMASS, or its equivalent system, as required by DoD guidance.

## (U) DoD CIO Has Not Fully Implemented Policies and Procedures to Reflect Updates Outlined in NIST SP 800-53, Revision 5

(U) The DoD CIO has not fully implemented the DoD's cybersecurity policies and procedures to reflect updates outlined in NIST SP 800-53, Revision 5. Revision 5 was issued in September 2020 and includes updates to 608 (60.4 percent) of the 1,007 controls. The updates include changes designed to limit the damage from cyber attacks, enhance system resiliency, and protect individual privacy. For example, specific to the metrics discussed in this management advisory (see the Appendix for a list of the six metrics), NIST SP 800-53, Revision 5:

*(U) NIST SP 800-53, Revision 5 updates include changes designed to limit the damage from cyber attacks, enhance system resiliency, and protect individual privacy.*

- (U) establishes a new set of controls related to SCRM, which requires the development of an organization-wide SCRM strategy, implementing guidance, and tools needed to consistently manage supply chain risks;

<sup>21</sup> (CUI) We reviewed eMASS to determine whether DoD officials indicated that they tested the information system contingency plan. Of the [REDACTED] systems, we identified that [REDACTED] systems had an ATO, but we did not obtain a copy of the contingency plans, testing documentation, or validate the information with the DoD Components.

- (U) adds controls related to privacy, which requires the development and periodically updating of an inventory of all programs and systems that process PII and to conduct PIAs to mitigate privacy-related risks; and
- (U) updates controls related to contingency planning, which requires the development of contingency plans and training.

(U) The OMB required Federal agencies to implement NIST SP 800-53, Revision 5 for all non-national security systems by September 2021, but as of December 2023, the DoD has not done so. In October 2023, the DoD CISO announced the adoption and transition timeline to implement the NIST SP 800-53, Revision 5 requirements. DoD OCIO officials explained that the DoD Components will adopt the updated controls before obtaining a new ATO using a phased approach over a 3-year period. Based on this timeline, the DoD Components will not fully implement the updated NIST requirements for all systems until 2026. In February 2024, DoD OCIO officials stated that the DoD RMF Knowledge Service and eMASS were updated to reflect the NIST SP 800-53, Revision 5 controls; however, the DoD OCIO still needs to develop the implementation guidance.

⋮ *(U) DoD Components will not  
fully implement the updated  
NIST requirements for all  
systems until 2026.*

(U) Until the DoD fully implements the updated NIST guidance into its policies and procedures, DoD officials are limited in their ability to operate at an effective level of security as defined by IG FISMA reporting metric guidance. Therefore,

the DoD CIO should issue interim guidance for non-national security systems, in coordination with the DoD CISO, for DoD Components to implement until DoD policy and procedures are updated to fully incorporate the NIST SP 800-53, Revision 5 requirements. The DoD CIO should also complete actions, in coordination with the DoD CISO, to fully incorporate the NIST SP 800-53, Revision 5 requirements into DoD policies and procedures, such as updating control information outlined in the RMF Knowledge Service and eMASS. In addition, the DoD CIO should implement a process, in coordination with the DoD CISO, to incorporate future NIST requirements into DoD policies and procedures for all DoD systems in a timely manner.



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

### **(U) Recommendation 1**

**(U) We recommend that the DoD Chief Information Officer:**

- a. **(U) Develop, in coordination with the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment, a DoD-wide Supply Chain Risk Management strategy as required by the National Institute of Standards and Technology guidance.**

### **(U) DoD Chief Information Officer Comments**

(U) The DoD CIO agreed, stating that they developed the DoD Information and Communications Technology and Services SCRM strategy to manage DoD-wide supply chain risks, which will be finalized by June 2024. The CIO also stated that they are actively participating in the development of the DoD-wide SCRM strategy, which is led by the Under Secretary of Defense for Acquisition and Sustainment.

### **(U) Our Response**

(U) Comments from the DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CIO issues the Information and Communications Technology SCRM strategy, the Under Secretary of Defense for Acquisition and Sustainment issues the DoD-wide SCRM strategy, and we verify that the strategies address the applicable SCRM-related NIST requirements.

- b. **(U) Develop, in coordination with the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment, policies and procedures implementing the DoD-wide Supply Chain Risk Management strategy as required by the National Institute of Standards and Technology guidance, including organizational-wide tools and techniques that allow DoD Components to consistently and effectively manage risks associated with using external providers.**

### **(U) DoD Chief Information Officer Comments**

(U) The DoD CIO agreed, stating that they updated DoD Instruction 5200.44 in February 2024 to provide guidance for managing risks associated with using external providers. The CIO explained that they are also implementing NIST SP 800-171 guidance in partnership with DoD Components to test commercial tools, develop techniques and capabilities to illuminate the supply chain, assess supplier cyber posture, and manage software and hardware assurance. Furthermore, the CIO stated that the DoD CISO formally adopted NIST SP 800-53, Revision 5, which includes SCRM-related controls.

### ***(U) Our Response***

(U) Comments from the DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once we verify that the updated DoD Instruction 5200.44 and the DoD-wide tools and techniques are designed to allow the DoD Components to consistently and effectively manage risks associated with using external providers, which implements the DoD-wide SCRM strategy as required by NIST guidance.

- c. **(U) Determine when DoD Components should complete a privacy impact assessment for information systems and ensure that all DoD guidance, including DoD Instruction 5400.16, “DoD Privacy Impact Assessment (PIA) Guidance,” July 14, 2015, Incorporating Change 1, August 11, 2017, and the DoD Risk Management Framework Knowledge Service guidance, aligns with that determination.**

### ***(U) DoD Chief Information Officer Comments***

(U) The DoD CIO agreed, stating that DoD Instruction 5400.16 outlines the requirements for completing PIAs, which must be reviewed and updated every 3 years or when a significant change occurs. The CIO explained in their response to Recommendation 1.d that they encouraged all system managers to complete a PIA for systems regardless of whether the system collects, maintains, uses, or disseminates PII; however, a full PIA is not required if the system does not have PII. The CIO further stated that DoD Instruction 5400.16 and the RMF Knowledge Service will be updated to address our recommendations.

### ***(U) Our Response***

(U) Comments from the DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CIO provides documentation showing that the reissued DoD Instruction 5400.16 and the updated DoD RMF Knowledge Service align with the CIO’s determination to require system managers to complete a full PIA for systems with PII or a shortened PIA for systems that do not have PII.

- d. **(U) Direct DoD Components, in coordination with the Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to require that officials conduct privacy impact assessments for all non-national security systems and update the Enterprise Mission Assurance Support Service, or its equivalent system, as required by DoD guidance.**

### ***(U) DoD Chief Information Officer Comments***

(U) The DoD CIO agreed, stating that they encourage all system managers to complete a PIA and obtain a program manager's signature. The CIO also stated that they will update DoD Instruction 5400.16 to require system managers to complete a PIA and conduct a privacy threat assessment for all systems.

### ***(U) Our Response***

(U) Comments from the DoD CIO partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. Although the CIO stated that they will update DoD Instruction 5400.16 to require PIAs for all systems, the CIO did not state whether they directed the DoD Components to conduct PIAs and update eMASS or its equivalent system. Therefore, we request that the DoD CIO provide additional comments within 30 days in response to the final advisory. The CIO's comments should describe their actions taken to direct DoD Components to conduct PIAs and update eMASS or its equivalent system.

- e. **(U) Implement a process, in coordination with the DoD Component Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, such as periodic Enterprise Mission Assurance Support Service reviews, to ensure that officials complete privacy impact assessments for all non-national security systems and update the Enterprise Mission Assurance Support Service, or its equivalent system, as required by DoD guidance.**

### ***(U) DoD Chief Information Officer Comments***

(U) The DoD CIO agreed, stating that they encourage all system managers to complete a PIA and obtain a program manager's signature. The CIO also said that they will update DoD Instruction 5400.16 to require system managers to complete a PIA and conduct a privacy threat assessment for all systems.

### ***(U) Our Response***

(U) Comments from the DoD CIO partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. Although the CIO stated that they will update DoD Instruction 5400.16 to require PIAs for all systems, the CIO did not state whether they planned to implement a process to ensure that DoD Components conducted PIAs and updated eMASS or its equivalent system. Therefore, we request that the DoD CIO provide additional comments within 30 days in response to the final advisory. The CIO's comments should describe their planned actions to ensure that DoD Components conducted PIAs and updated eMASS, or its equivalent system, as required by DoD guidance.

- f. **(U) Direct DoD Components, in coordination with the Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to conduct business impact analyses for all non-national security systems and update the Enterprise Mission Assurance Support Service, or equivalent system, as required by DoD guidance.**

***(U) DoD Chief Information Officer Comments***

(U) The DoD CIO agreed, stating that they will direct DoD Components to conduct BIAs for all non-national security systems and update eMASS or other authoritative RMF inventory tool. The CIO explained that they will add BIA metrics to the Cyber Hardening Scorecard using data fields from eMASS and manual entries from DoD Components not using eMASS. The CIO also stated that the DoD Components can track the progress of the BIA metrics during monthly pre-CISO Scorecard reviews.

***(U) Our Response***

(U) Comments from the DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CIO provides documentation demonstrating that they directed DoD Components to conduct BIAs for all non-national security systems and updated eMASS, or its equivalent system, and that the DoD Components performed reviews of the BIA metrics during their monthly pre-CISO Scorecard meetings.

- g. **(U) Implement a process, in coordination with the Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, such as periodic Enterprise Mission Assurance Support Service reviews, to ensure that DoD officials complete business impact analyses for all non-national security systems and update the Enterprise Mission Assurance Support Service, or its equivalent system, as required by DoD guidance.**

***(U) DoD Chief Information Officer Comments***

(U) The DoD CIO agreed, stating that the RMF Technical Advisory Group Chair and Secretariat will coordinate with the RMF Technical Advisory Group and the AO Council communities to set up an annual review of the BIA information found in eMASS. The CIO explained that the RMF Technical Advisory Group Secretariat will update the RMF Knowledge Service site with BIA guidance and best practices.

### ***(U) Our Response***

(U) Comments from the DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CIO provides documentation demonstrating that the RMF Technical Advisory Group updated the RMF Knowledge Service site with BIA guidance and conducted an annual review of the BIA information found in the eMASS.

- h. (U) Direct DoD Components, in coordination with the Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to conduct information system contingency plan testing, including annual tests, for all non-national security systems and update the Enterprise Mission Assurance Support Service, or its equivalent system, as required by DoD guidance.**

### ***(U) DoD Chief Information Officer Comments***

(U) The DoD CIO agreed, stating that they have directed DoD Components to conduct information system contingency plan testing, including annual tests, for all non-national security systems and update eMASS, or its equivalent system, as required by the Committee on National Security Systems and NIST guidance. The CIO also stated that they will add metrics to the Cyber Hardening Scorecard to track the information system contingency plan testing.

### ***(U) Our Response***

(U) Comments from the DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CIO provides documentation demonstrating that they directed DoD Components to complete contingency plan testing for all non-national security systems and update the eMASS, or its equivalent system, and tracked information system contingency plan testing on the Cyber Hardening Scorecard.

- i. (U) Implement a process, in coordination with the Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, such as periodic Enterprise Mission Assurance Support Service reviews, to ensure that DoD officials annually test contingency plans for all non-national security systems and update the status of the tests in Enterprise Mission Assurance Support Service, or its equivalent system, as required by DoD guidance.**



### ***(U) DoD Chief Information Officer Comments***

(U) The DoD CIO agreed, stating that they have directed DoD Components to conduct information system contingency plan testing, including annual tests, for all non-national security systems and update eMASS, or its equivalent system, as required by the Committee on National Security Systems and NIST guidance. The CIO also stated that they will add metrics to the Cyber Hardening Scorecard to track the information system contingency plan testing.

### ***(U) Our Response***

(U) Comments from the DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CIO provides documentation demonstrating that they tracked information system contingency plan testing on the Cyber Hardening Scorecard.

- j. **(U) Issue interim guidance for non-national security systems, in coordination with the Chief Information Security Officer, for DoD Components to implement until DoD policy and procedures are updated to fully incorporate the National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5, Updated December 2020, requirements.**

### ***(U) DoD Chief Information Officer Comments***

(U) The DoD CIO agreed, stating that the DoD CISO issued an October 2023 memorandum that serves as the announcement of the DoD's adoption and transition timeline for the NIST SP 800-53, Revision 5 controls and the corresponding control baseline guidance from the Committee on National Security Systems.

### ***(U) Our Response***

(U) Comments from the DoD CIO addressed the specifics of the recommendation. The CIO explained that the October 2023 DoD CISO memorandum serves as the DoD's guidance for adopting the NIST SP 800-53, Revision 5 controls. The CIO also stated in their response to Recommendation 1.k that they updated eMASS to include the NIST SP 800-53, Revision 5 control information, with a migration functionality for existing systems in February 2024. Therefore, the recommendation is closed, and no further comments are required.

- k. **(U) Complete actions, in coordination with the Chief Information Security Officer, to fully incorporate the National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5, Updated December 2020, requirements into DoD policies and procedures, such as updating control information outlined in the Risk Management Framework Knowledge Service and the Enterprise Mission Assurance Support Service.**

### ***(U) DoD Chief Information Officer Comments***

(U) The DoD CIO agreed, stating that they updated the RMF Knowledge Service in January 2024 to provide the NIST SP 800-53, Revision 5 control information. The CIO also stated that they updated eMASS to include the control information in August 2023, but the migration functionality for existing systems was not available until February 2024.

### ***(U) Our Response***

(U) Comments from the DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. Although the CIO updated the NIST SP 800-53, Revision 5 control information for RMF Knowledge Service and provided the migration functionality for existing systems in eMASS, the CIO still needs to develop the implementation guidance as part of the RMF Knowledge Service, such as the common body of evidence that DoD Components will use to support their security control assessments as part of the ATO process. We will close the recommendation once the CIO provides documentation demonstrating that they issued the common body of evidence for DoD Components to use when implementing NIST SP 800-53, Revision 5.

- l. **(U) Implement a process, in coordination with the Chief Information Security Officer, to incorporate future National Institute of Standards and Technology requirements into DoD policies and procedures for all DoD systems in a timely manner.**

### ***(U) DoD Chief Information Officer Comments***

(U) The DoD CIO agreed, stating that they will continue to follow the current process for policy updates, adhering to the established DoD Issuance Program timelines. The CIO also stated that they intend to wait for updated guidance from the Committee on National Security Systems before revising DoD policy and procedures on updated NIST guidance for all DoD systems.

### *(U) Our Response*

~~(CUI)~~ Comments from the DoD CIO did not address the specifics of the recommendation; therefore, the recommendation is unresolved. As stated in this advisory, we identified that it took the DoD CIO more than 3 years to adopt NIST SP 800-53, Revision 5 while waiting for the Committee on National Security Systems to provide its update for guidance relating to national security systems. This process will not be fully implemented until 2026, which will result in unnecessary delays in issuing DoD guidance for implementing NIST SP 800-53, Revision 5 controls for [REDACTED] of non-national security systems.<sup>22</sup> While waiting for the Committee on National Security Systems guidance, the CIO could have provided interim guidance to the DoD Components to use for their non-national security systems, which could have reduced the timeframe for fully implementing the NIST SP 800-53, Revision 5 controls for all DoD systems. Therefore, we request that the DoD CIO provide additional comments within 30 days in response to the final advisory. The CIO's comments should describe their planned actions to establish a process to incorporate future, updated NIST guidance in a timely manner.

---

<sup>22</sup> ~~(CUI)~~ As a result, we identified [REDACTED] non national security systems with an ATO in eMASS as of May 2023.

## (U) Appendix

### (U) FISMA Reporting Metric Updates

(U) 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.<sup>23</sup> Specifically, the OMB made the following changes to the IG FISMA reporting process in OMB Memorandum M-22-05.<sup>24</sup>

- (U) Shifted the annual due date for the IG FISMA reporting from October to July to better align the release of the IG results with the development of the President’s Budget.
- (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.

(U) As part of the new multiyear review cycle, IGs are required to report annually on the 20 Core metrics and the remaining 37 Supplemental metrics are assessed over a 2-year cycle.<sup>25</sup> 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. For FY 2024, IGs will report on 37 metrics—20 Core and 17 Supplemental.<sup>26</sup>

### (U) Assigning IG Metric Ratings

(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

<sup>23</sup> (U) Executive Order 14028, “Improving the Nation’s Cybersecurity,” May 12, 2021.

<sup>24</sup> (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.

<sup>25</sup> (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 you remove 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.

<sup>26</sup> (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) 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. Figure 1 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 1. IG FISMA Maturity Model



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

## (U) Scope and Methodology

(U) We assessed the 40 metrics (20 Core and 20 Supplemental) of the DoD's information security program and practices as part of our FY 2023 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, the Department of Homeland Security, and the DoD OCIO on July 31, 2023. We explained our rationale for each rating in the response to the summary metric questions for each of the 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 2023 FISMA review for selected metrics and to issue recommendations for corrective action. Of the 40 assessed metrics that we assessed as part of our FY 2023 review, we are reporting on 6 metrics—3 Core and 3 Supplemental—that represent three of the nine domains. We use a risk-based approach for selecting the metrics to report on each year. Table 2 lists the six metrics we are reporting on in this advisory.

(U) Table 2. IG FISMA Reporting Metrics Assessed

(U) FISMA Function ( <i>Domain</i> )	Metric No.	Metric Type	Metric Question
Identify ( <i>SCRM</i> )	12	FY 2023 Supplemental	To what extent does the organization use an organization wide SCRM strategy to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?
Identify ( <i>SCRM</i> )	13	FY 2023 Supplemental	To what extent does the organization use SCRM policies and procedures to manage SCRM activities at all organizational tiers?
Identify ( <i>SCRM</i> )	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?
Protect ( <i>Data Protection and Privacy</i> )	35	FY 2023 Supplemental	To what extent has the organization developed a privacy program for the protection of PII that is collected, used, maintained, shared, and disposed of by information systems?
Recover ( <i>Contingency Planning</i> )	61	Core	To what extent does the organization ensure that the results of BIAs are used to guide contingency planning efforts?
Recover ( <i>Contingency Planning</i> )	63	Core	To what extent does the organization perform tests/ exercises of its information system contingency planning processes?

(U)

(U) Source: The DoD OIG.

(U) In addition to reporting on the six metrics, we also are reporting on the need for the DoD to revise its policies and procedures to reflect updates in NIST SP 800-53, Revision 5, which includes changes to 608 of the 1,007 controls (60.4 percent). NIST defines a change as anything that impacts the implementation, testing, or security documentation required for the control.

(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 sensitive information, other management reports supporting the DoD's efforts to oversee the implementation of selected 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) Defense Information Systems Agency;
- (U) U.S. Cyber Command; and
- (U) Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency.

(U) This report was reviewed by the DoD Component associated with this oversight 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. In preparing and marking this advisory, we considered any comments submitted by the DoD Component about the CUI treatment of their information. If the DoD component failed to provide any or sufficient comments about the CUI treatment of their information, we marked this advisory based on our assessment of the available information.

# (U) Management Comments

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



CHIEF INFORMATION OFFICER

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

APR 3 2024

### MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

**SUBJECT:** Review and Comment of DoD Inspector General “Draft Management Advisory: The DoD’s FY 2023 Compliance with the Federal Information Security Modernization Act of 2014 (Project No. D2023-D000CP-0026.001)”

This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the draft DoD Inspector General Report, “Draft Management Advisory: The DoD’s FY 2023 Compliance with the Federal Information Security Modernization Act of 2014 (Project No. D2023-D000CP-0026.001):

**DoD IG RECOMMENDATION 1.a:** We recommend that the DoD Chief Information Officer develop, in coordination with the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment, a DoD-wide Supply Chain Risk Management strategy as required by the National Institute of Standards and Technology guidance.

**DoD CIO RESPONSE 1.a:** DoD CIO agrees with the DoD IG recommendation.

The DoD CIO developed the DoD Strategy and Implementation Plan for Information and Communications Technology and Services (ICTS) Supply Chain Risk Management Assurance to manage risk in the Department’s ICTS supply chain (ICT-SCRM Strategy). The ICT-SCRM Strategy was developed in coordination with stakeholders across the Department, and formal staffing is nearing completion. DoD CIO forecasts signing the ICT-SCRM Strategy in the third quarter of fiscal year 2024. Further, CIO actively participates in the implementation of the DoD SCRM Framework, a multi-phase effort led by the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) which will include developing an overarching SCRM strategy for the DoD. CIO leads Lines of Effort 5 and 6 (Cyber SCRM and ICT SCRM) within the USD(A&S)-led DoD SCRM Framework.

**DoD IG RECOMMENDATION 1.b:** We recommend that the DoD Chief Information Officer develop, in coordination with the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment, policies and procedures implementing the DoD-wide Supply Chain Risk Management strategy as required by the National Institute of Standards and Technology guidance, including organizational-wide tools and techniques that allow DoD Components to consistently and effectively manage risks associated with using external providers.

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

The DoD CIO, in coordination with the Under Secretary of Defense for Research and Engineering (USD(R&E)), signed the Department of Defense Instruction 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks” on February 16, 2024, providing guidance on managing risks associated with using external providers. In partnership with DoD Components (to include USD(A&S) and USD(R&E)), CIO is implementing National

## (U) Chief Information Officer of The Department of Defense (cont'd)

Institute of Standards and Technology (NIST) guidance in Special Publication (SP) 800-171 and experimenting with commercial tools, developing techniques and capability to illuminate the supply chain, assess supplier cyber posture, manage software and hardware assurance. Additionally, the DoD Chief Information Security Officer formally adopted the NIST SP 800-53 revision 5 which included the supply chain risk management family of controls, such as a SCRM Plan; Supply Chain Controls; Processes, Provenance, Supplier Assessments and Reviews; Tamper Resistance and Detection; and others.

**DoD IG RECOMMENDATION 1.c:** We recommend that the DoD Chief Information Officer determine when DoD Components should complete a privacy impact assessment for information systems and ensure that all DoD guidance, including DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, Incorporating Change 1, August 11, 2017, and the DoD Risk Management Framework Knowledge Service guidance, aligns with that determination.

**DoD CIO RESPONSE 1.c:** DoD CIO agrees with the DoD IG recommendation.

The DoDI 5400.16 outlines that PIAs must be reviewed and updated every three years and/or when a significant change to a system or a change in privacy or security posture occurs. Additional updates will be made to ensure DoD IG's recommendations are appropriately addressed. The Risk Management Framework Knowledge Service (RMF KS) will be updated appropriately.

**DoD IG RECOMMENDATION 1.d:** We recommend that the DoD Chief Information Officer direct DoD Components, in coordination with the Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to require that officials conduct privacy impact assessments for all non-national security systems and update the Enterprise Mission Assurance Support Service, or its equivalent system, as required by DoD guidance.

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

DoD PIA policy, DoDI 5400.16, currently outlines PIA requirements and is being updated to ensure DoD IG's recommendations are appropriately addressed.

We encourage all system managers to complete a PIA, however, if a system does not collect, maintain, use, or disseminate personally identifiable information (PII), a full PIA is not required. System managers need only to complete the main information for the PIA, mark "no information is collected," and obtain program manager signature. This policy will be set forth in the upcoming reissuance of DoDI 5400.16, which will also include the requirement that a Privacy Threat Assessment (PTA) is conducted on all systems as discussed in NIST SP 800-53.

**DoD IG RECOMMENDATION 1.e:** We recommend that the DoD Chief Information Officer implement a process, in coordination with the DoD Component Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, such as periodic Enterprise Mission Assurance Support Service reviews, to ensure that officials complete privacy impact assessments for all non-national security systems and update the Enterprise Mission Assurance Support Service, or its equivalent system, as required by DoD guidance.

## (U) Chief Information Officer of The Department of Defense (cont'd)

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

DoD PIA policy, DoDI 5400.16, currently outlines PIA requirements and is being updated to ensure DoD IG's recommendations are appropriately addressed.

We encourage all systems to complete a PIA however, if the system does not collect, maintain, use, or disseminate PII, a full PIA is not required. They only need to complete the main information, mark "no information is collected," and obtain program manager signature. This will be directly expressed in the upcoming reissuance of DoDI 5400.16, and this will ensure a PTA is conducted on all systems as discussed in NIST SP 800-53.

**DoD IG RECOMMENDATION 1.f:** We recommend that the DoD Chief Information Officer direct DoD Components, in coordination with the Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to conduct business impact analyses for all non-national security systems and update the Enterprise Mission Assurance Support Service, or equivalent system, as required by DoD guidance.

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

The DoD CIO will direct DoD Components, in coordination with the Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to conduct business impact analyses for all non-national security systems and update Enterprise Mission Assurance Support Service (eMASS), or other authoritative RMF Inventory Tool. This will be done by adding metrics on business impact analyses to the Cyber Hardening Scorecard (CHS) using data fields in eMASS and manual entries from Components not using eMASS. The CHS will be reviewed by Components at the monthly Pre-CISO Scorecard review meeting where the members/participants can track progress.

**DoD IG RECOMMENDATION 1.g:** We recommend that the DoD Chief Information Officer implement a process, in coordination with the Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, such as periodic Enterprise Mission Assurance Support Service reviews, to ensure that DoD officials complete business impact analyses for all non-national security systems and update the Enterprise Mission Assurance Support Service, or its equivalent system, as required by DoD guidance.

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

The RMF TAG Chair and Secretariat will coordinate with the RMF TAG and Authorizing Official Council communities to set up an annual review of business impact analyses (BIA) information found in the eMASS. Additionally, the RMF TAG Secretariat will update the RMF KS site with BIA guidance and best practices. This guidance will be coordinated for approval with the RMF TAG and Authorizing Official Council per charter guidelines.

**DoD IG RECOMMENDATION 1.h:** We recommend that the DoD Chief Information Officer direct DoD Components, in coordination with the Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to conduct information system contingency plan testing, including annual tests, for all non-national security systems and update the Enterprise Mission Assurance Support Service, or its equivalent system, as required by DoD guidance.



## (U) Chief Information Officer of The Department of Defense (cont'd)

### **DoD CIO RESPONSE 1.h:** DoD CIO agrees with the DoD IG recommendation.

The DoD CIO has directed DoD Components, in coordination with the Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to conduct information system contingency plan testing, including annual tests, for all non-national security systems and update Enterprise Mission Assurance Support Service (eMASS), or its equivalent system. This is required by the Committee on National Security Systems Instruction (CNSSI) 1253, "Security Categorization and Control Selection for National Security System" and the NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations" as part of security control CP-4, "Contingency Plan Testing" and its associated Enterprise Assignment Values. This control will be tracked via metrics added to the Cyber Hardening Scorecard.

**DoD IG RECOMMENDATION 1.i:** We recommend that the DoD Chief Information Officer implement a process, in coordination with the Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, such as periodic Enterprise Mission Assurance Support Service reviews, to ensure that DoD officials annually test contingency plans for all non-national security systems and update the status of the tests in Enterprise Mission Assurance Support Service, or its equivalent system, as required by DoD guidance.

### **DoD CIO RESPONSE 1.i:** DoD CIO agrees with the DoD IG recommendation.

The DoD CIO has directed DoD Components, in coordination with the Chief Information Security Officers, Chief Information Officers, and Authorizing Officials, to conduct information system contingency plan testing, including annual tests, for all non-national security systems and update eMASS, or its equivalent system, as required per CNSSI 1253 and NIST SP 800-53 as part of security control CP-4 and its associated Enterprise Assignment Values. This control will be tracked via metrics added to the Cyber Hardening Scorecard.

**DoD IG RECOMMENDATION 1.j:** We recommend that the DoD Chief Information Officer issue interim guidance for non-national security systems, in coordination with the Chief Information Security Officer, for DoD Components to implement until DoD policy and procedures are updated to fully incorporate the National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5, Updated December 2020, requirements.

### **DoD CIO RESPONSE 1.j:** DoD CIO agrees with the DoD IG recommendation.

The DoD Chief Information Security Officer issued a memorandum, "Adoption of NIST SP 800-53 and CNSSI 1253 Revision 5," on October 16, 2023, which serves as an announcement of the Department's adoption and transition timeline for Revision 5 of the NIST SP 800-53 security controls and the corresponding control baselines in Revision 5 of the CNSSI 1253.

**DoD IG RECOMMENDATION 1.k:** We recommend that the DoD Chief Information Officer complete actions, in coordination with the Chief Information Security Officer, to fully incorporate the National Institute of Standards and Technology Special Publication 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 5, Updated December 2020, requirements into DoD policies and procedures, such as updating control information outlined in the Risk Management Framework Knowledge Service and the Enterprise Mission Assurance Support Service.

## (U) Chief Information Officer of The Department of Defense (cont'd)

**DoD CIO RESPONSE 1.k:** DoD CIO agrees with the DoD IG recommendation.

The DoD CIO completed the update to the RMF Knowledge Service on January 24, 2024, to provide control information for CNSSI 1253 Rev 5 and NIST SP 800-53 Rev 5 controls. The updated control information was made available in eMASS for new systems in August 2023, with migration functionality for existing systems available in February 2024.

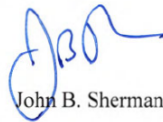
**DoD IG RECOMMENDATION 1.i:** We recommend that the DoD Chief Information Officer implement a process, in coordination with the Chief Information Security Officer, to incorporate future National Institute for Standards and Technology requirements into DoD policies and procedures for all DoD systems in a timely manner.

**DoD CIO RESPONSE 1.i:** DoD CIO agrees with the DoD IG recommendation.

Incorporation of future NIST standards into DoD policies and procedures for all DoD systems will continue to follow the current process which includes adhering to the WHS DoD Issuance Program timelines for policy updates or, in the case of NIST SP 800-53, after CNSSI 1253 updates have been published to reflect updated NIST standards.

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

The point of contact for this matter is [REDACTED]



John B. Sherman

CUI



CUI

## **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 <http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/> or contact the Whistleblower Protection Coordinator at [Whistleblowerprotectioncoordinator@dodig.mil](mailto: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](mailto:public.affairs@dodig.mil); 703.604.8324

### **DoD OIG Mailing Lists**

[www.dodig.mil/Mailing-Lists/](http://www.dodig.mil/Mailing-Lists/)



[www.twitter.com/DoD\\_IG](https://www.twitter.com/DoD_IG)

### **LinkedIn**

<https://www.linkedin.com/company/dod-inspector-general/>

### **DoD Hotline**

[www.dodig.mil/hotline](http://www.dodig.mil/hotline)



**CUI**



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive  
Alexandria, Virginia 22350-1500  
[www.dodig.mil](http://www.dodig.mil)  
DoD Hotline 1.800.424.9098

**CUI**