U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

FEDERAL INFORMATION SECURITY MODERNIZATION ACT AUDIT FISCAL YEAR 2025

Report Number 2025-ISAG-008
November 24, 2025

EXECUTIVE SUMMARY

Federal Information Security Modernization Act Audit - Fiscal Year 2025

Report No. 2025-ISAG-008 **November 24, 2025**

Why Did We Conduct the Audit?

Our overall objective was to evaluate the U.S. Office of Personnel Management's (OPM) security program and practices, as required by the Federal Information Security Modernization Act (FISMA) of 2014. Specifically, we reviewed the status of OPM's information technology security program in accordance with the U.S. Department of Homeland Security's (DHS) FISMA Inspector General Reporting Metrics.

What Did We Audit?

The OPM Office of the Inspector General has completed a performance audit of OPM's general FISMA compliance efforts in the areas defined in DHS's guidance and the corresponding reporting instructions. Our audit was conducted from December 2024 through August 2025 at OPM headquarters in Washington, D.C.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

The FISMA Inspector General reporting metrics uses a maturity model evaluation system derived from the National Institute of Standards and Technology's Cybersecurity Framework. The Cybersecurity Framework is comprised of 10 "domain" areas and the weighted averages of the domain scores are used to derive the agency's overall cybersecurity score. In fiscal year 2025, OPM's cybersecurity maturity level is measured as "2 – *Defined*."

The following sections provide a high-level outline of OPM's performance in each of the 10 domains from the 6 cybersecurity framework functional areas:

Cybersecurity Governance – OPM consistently implements its risk management strategies at the organizational, mission/business process, and system levels. OPM also calculates, documents, categorizes and prioritizes cybersecurity risks. However, OPM does not evaluate and adjust its cybersecurity risk management strategies based on its threat environment and risk assessments.

Cybersecurity Supply Chain Risk – OPM has developed and maintains a Cybersecurity Supply Chain Risk Management (C-SCRM) Strategy that defines OPM's C-SCRM requirements and processes, including acquisition and contractual security measures.

Risk and Asset Management – OPM is in the process of developing an enterprise software inventory list. However, due to the cancellation of the Enterprise Software Registry project, OPM has not completed documenting the processes and procedures for developing and maintaining the software inventory list.

Configuration Management – OPM has developed policies and procedures for ensuring that configuration settings/common secure configurations are defined, implemented, and monitored for the majority of its systems. However, the agency has not established configuration settings/common secure configurations for all systems in its environment

Identity And Access Management – OPM has defined and implemented strong, multi-factor authentication mechanisms for non-privileged users of the organization's physical and logical assets, including remote access to networks. Additionally, public facing systems consistently support phishing resistant multi-factor authentication.

Data Protection and Privacy – OPM has developed policies and procedures for data exfiltration, endpoint detection and response, enhanced network defenses, email authentication, and Domain Name System tampering. However, we found that the policies and procedures have not been consistently implemented as it relates to their security logging capabilities. OPM is not capturing/ingesting logs into its security information and event management system for investigative purposes.

Security Training – OPM has defined its process for assessing the knowledge, skills, and abilities of its workforce to determine its specialized training needs and periodically updating its assessment to account for a changing risk environment. Further, the organization has also assessed the knowledge, skills, and abilities of its workforce and has identified skills gaps.

However, OPM has not utilized the results of its workforce assessment and skills gap analysis to update its awareness and training strategies or plans required by OPM's Implementation Procedures and Guidelines: Awareness and Training policy.

Information Security Continuous Monitoring – OPM's continuous monitoring strategy addresses security control monitoring at the organization and business units. However, information security continuous monitoring testing revealed 35 systems have over 740 IT security controls that are partially or are not satisfied, whereas only 208 plan of action and milestones are open to monitor risks.

Incident Response – The OIG examined 55 FISMA systems that should be at a minimum of Event Logging (EL) Tier 1 (Basic), which requires an organization to meet logging requirements of highest criticality including logging categories, a time standard, and basic centralized access. However, 19 systems do not meet EL1 logging requirements.

Contingency Planning – OPM has defined its policies, procedures, and processes for information system contingency plan (ISCP) testing and exercises. Additionally, OPM has implemented and conducted routine ISCP testing to ensure that critical systems can be recovered within established timeframes after a disruption or disaster. However, our testing found that six ISCP tests have exceeded the annual update deadlines. Two of those six are high value asset systems.

ABBREVIATIONS

CIGIE	Council of the Inspectors General on Integrity and Efficiency
C-SCRM	Cybersecurity Supply Chain Risk Management
DHS	U.S. Department of Homeland Security
EL	Event Logging
ERM	Enterprise Risk Management
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
IG	Inspector General
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NFR	Notice of Findings and Recommendations
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OESPIM	Office of the Executive Secretariat, Privacy, and Information Management
OIG	Office of the Inspector General
OMB	U.S. Office of Management and Budget
OPM	U.S. Office of Personnel Management
POA&M	Plan of Action and Milestones
SP	Special Publication

TABLE OF CONTENTS

I. BACKGROUND

The 2002 Federal Information Security Management Act (FISMA) required (1) annual agency program reviews, (2) annual Inspector General evaluations, (3) agency reporting to the U.S. Office of Management and Budget (OMB) on the results of Inspector General evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In 2014, FISMA reemphasizes the need for an annual Inspector General evaluation. In accordance with FISMA, we conducted an audit of the U.S. Office of Personnel Management (OPM)'s security program and practices. As part of our audit, we reviewed OPM's FISMA compliance strategy and documented the status of its compliance efforts.

FISMA requirements pertain to all information systems supporting the operations and assets of an agency, including those systems currently in place or planned. The requirements also pertain to information technology (IT) resources owned and/or operated by a contractor supporting agency systems.

FISMA reaffirms the Chief Information Officer's strategic agency-wide security responsibility. At OPM, security responsibility is assigned to the agency's Office of the Chief Information Officer (OCIO). FISMA also clearly places responsibility on each agency's OCIO to develop, implement, and maintain a security program that assesses risk and provides adequate security for the operations and assets of programs and systems under its control.

To assist agencies and Inspectors General in fulfilling their FISMA evaluation and reporting responsibilities, the U.S. Department of Homeland Security (DHS) Office of Cybersecurity and Communications issued the Inspector General FISMA Reporting Metrics. This document provides a methodology and format for agencies to report FISMA audit results to DHS. It identifies a series of reporting topics that relate to specific agency responsibilities outlined in FISMA.

The Council of the Inspectors General on Integrity and Efficiency, OMB, and DHS developed the FISMA Inspector General Reporting Metrics utilizing a maturity model evaluation system derived from the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Our audit and reporting approaches were designed in accordance with the issued guidance.

II. OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

Our overall objective was to evaluate OPM's security program and practices, as required by FISMA. Specifically, we reviewed the status of the following areas of OPM's IT security program in accordance with DHS's FISMA IG reporting requirements:

- Cybersecurity Governance;
- Cybersecurity Supply Chain Risk Management;
- Risk and Asset Management;
- Configuration Management;
- Identity and Access Management;
- Data Protection and Privacy;
- Security Training;
- Information Security Continuous Monitoring;
- Incident Response; and
- Contingency Planning.

We are also performing an audit focused on one of OPM's major information systems – FOIA Xpress.

SCOPE AND METHODOLOGY

We conducted this performance audit in accordance with the U.S. Government Accountability Office's Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit covered OPM's FISMA compliance efforts throughout fiscal year (FY) 2025.

Like prior years, we requested that OPM conduct a self-assessment. This self-assessment gave OPM the opportunity to document its current maturity level for each metric and the maturity level that it hoped to achieve by the end of the following year, FY 2026. We validated OPM's stated/current maturity level throughout the fiscal year and reported on the results of our

analysis. Recommendations were made to help OPM attain the desired maturity level if it was higher than the IG assessed maturity level.

We reviewed OPM's general FISMA compliance efforts in the specific areas defined in DHS's guidance and the corresponding reporting instructions. We considered the internal control structure for various OPM systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls for these various systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. We utilized this understanding to evaluate the degree to which the appropriate internal controls were designed and implemented. As appropriate, we conducted compliance tests using judgmental samples to determine the extent to which established controls and procedures are functioning as required. The results of the judgmentally selected sample were not projected to the population since it is unlikely that the results are representative of the population.

In conducting our audit, we relied on varying degrees of computer-generated data provided by OPM. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. However, we believe that the data was sufficient to achieve the audit objectives, and nothing came to our attention during our audit to cause us to doubt its reliability.

Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the set of internal controls for these various systems taken as a whole.

The criteria used in conducting this audit included:

- NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations;
- NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy;
- OPM Implementation Procedures and Guidelines: System and Communications Protection;
- OPM's Implementation Procedures and Guidelines: System and Information Integrity;
- OMB Memorandum M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents;
- OPM Information Technology Security FISMA Procedures;

- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- NIST Cybersecurity Framework 2.0; and
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations.

The OPM Office of the Inspector General (OIG), established by the Inspector General Act of 1978, as amended, performed the audit from December 2024 through August 2025 in OPM's Washington, D.C. office.

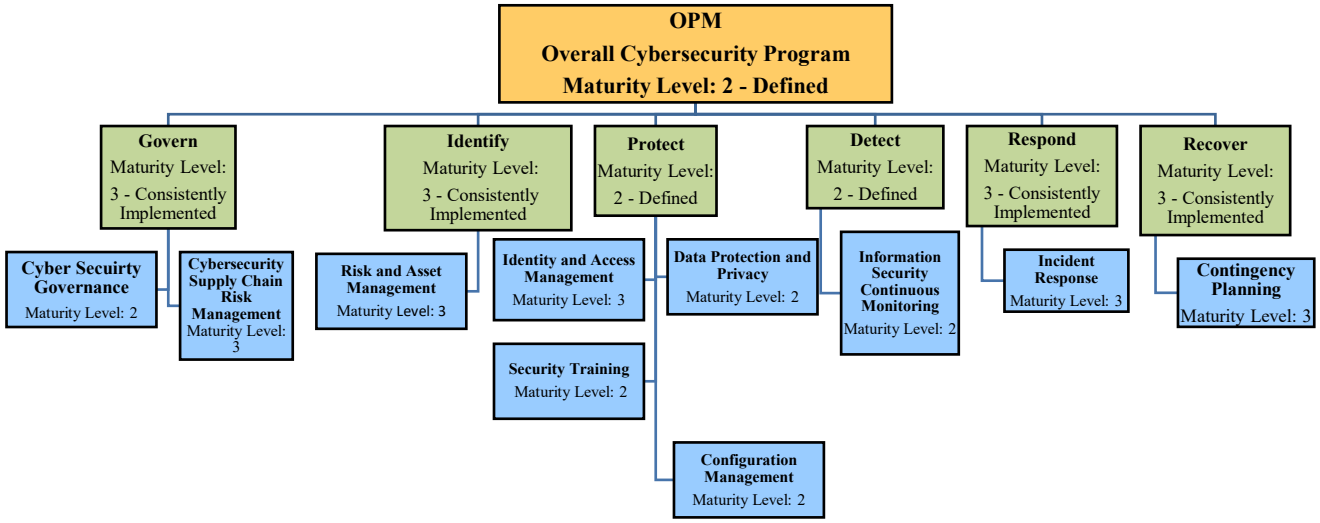
COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether OPM's practices were consistent with applicable standards. While generally compliant with respect to the items tested, OPM's OCIO and other program offices were not in complete compliance with all standards, as described in Section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. INTRODUCTION AND OVERALL ASSESSMENT

The FISMA Inspector General Reporting Metrics use a maturity model evaluation system derived from the NIST Cybersecurity Framework. In FY 2024, the Cybersecurity Framework was comprised of 5 "function" areas that mapped to the 9 "domains" under the function areas. In FY 2025, the Cybersecurity Framework is comprised of 6 "function" areas that map to the 10 "domains" under the function areas. These 10 domains are broad cyber security control areas used to assess the effectiveness of the information security policies, procedures, and practices of the agency. Each domain is comprised of a series of individual metrics, which are the specific controls that we evaluated and tested when assessing the agency's cybersecurity program. Each metric receives a maturity level rating of 1-5. The chart below outlines the overall maturity of OPM's cybersecurity program.



The following table outlines the description of each maturity level rating, as defined by the Inspector General FISMA Reporting Metrics:

Maturity Level	Maturity Level Description
Level 1: *Ad Hoc*	Policies, procedures, and strategy are not formalized; activities are performed in an ad hoc, reactive manner.
Level 2: *Defined*	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: *Consistently Implemented*	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.

Maturity Level	Maturity Level Description
Level 4: *Managed and Measurable*	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary
Level 5: *Optimized*	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology

In previous years, inspectors general have been directed to utilize a mode-based scoring approach to assess agency maturity levels. Under this approach, ratings throughout the reporting domains were determined by a simple majority, where the most frequent level (i.e., the mode) across the questions served as the domain rating. The same logic was applied to the function and overall information security program level. However, in FY 2021, OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) conducted a pilot to score agencies based on a weighted average for certain priority metrics. One purpose of this pilot was to help evaluate the impacts of these priority metrics and prepare agencies for the possibility of changing the maturity calculation process in the future.

Through analysis of the data obtained from this pilot and the FY 2020 – FY 2022 government-wide Inspector General FISMA reporting, OMB and CIGIE determined that a non-weighted (e.g., calculated) average more closely aligned with the OIG's assessed maturity levels expressed in a numeric format. Therefore, ratings in FY 2025 were based on a calculated average approach, wherein the average of the metrics in a particular domain was used by IGs to determine the effectiveness of individual function areas (*govern, identify*, *protect*, *detect*, *respond*, and *recover*) and the overall program.

There are two distinct groups of metrics: Core and Supplemental. Core Metrics are assessed annually and represent administration priorities, high impact security processes, and essential functions necessary to determine OPM's security program effectiveness. Supplemental Metrics are assessed once every two years and demonstrate activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness. The OPM OIG evaluates all metrics each year. The following table provides the scores, both weighted average and calculated average, as well as each function area for both core and supplemental metrics.

2025 FISMA Metrics Results

Function	Core	FY 2025 Supplemental	FY 2025 Weighted Average	FY 2025 Calculated Average	FY 2025 Assessed Maturity
Govern	3.00	2.00	2.14	2.50	Consistently Implemented (Level 3)
Identify	3.20	1.00	2.60	2.83	Consistently Implemented (Level 3)
Protect	2.25	N/A	2.25	2.13	Defined (Level 2)
Detect	2.00	2.00	2.00	2.00	Defined (Level 2)
Respond	3.00	N/A	3.00	3.00	Consistently Implemented (Level 3)
Recover	2.5	N/A	2.67	2.5	Consistently Implemented (Level 3)
Overall Maturity	**2.66**	**1.67**	**2.44**	**2.49**	**Defined (Level 2)**

The remaining sections of this report provide the detailed results of our audit. Sections B through J outline how we rate the maturity level of each individual metric, which ultimately determined the agency's maturity level for each domain and function.

B. CYBERSECURITY GOVERNANCE

Cybersecurity Governance controls allow OPM to incorporate cybersecurity into its broader enterprise risk management strategy and address an understanding of organizational context; the establishment of cybersecurity strategy and cybersecurity supply chain risk management; roles, responsibilities, and authorities; policy; and the oversight of cybersecurity strategy.

The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Cybersecurity Governance domain is "2 – *Defined*."**

Metric 1 - Cybersecurity Profiles

FY 2025 Maturity Level: 1 – Ad Hoc. OPM has developed and maintains its current and target cybersecurity profiles, which describe OPM's current cybersecurity status and goals. However, OPM has not defined its policies and procedures, including the organization's mission objectives, threat landscape, resources (including personnel), and constraints.

OPM does not have policies and procedures for their cybersecurity profiles.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Consistently Implemented*. We have assessed this metric as *Ad Hoc*. The recommendation below is to assist OPM with attaining the *Defined* maturity level.

NIST SP 800-53, Revision 5, Control PM-11 states that organizations should "Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and … Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and … Review and revise the mission and business processes [Assignment: organization-defined frequency]."

Failure to establish policies and procedures for developing and maintaining OPM's cybersecurity profiles increases the likelihood that the profiles are improperly created and maintained and thus less effective in reducing risks in OPM's environment.

Recommendation 1

We recommend that OPM update the Enterprise Risk Management Strategy and Process Guide to accurately reflect the development and maintenance of OPM's cybersecurity profiles.

OPM Response

"Non-Concur. The draft NFR* [Notice of Findings and Recommendations] *reads 'however, OPM lacked supporting documentation for the development and maintenance of the current and target profiles that includes OPM's mission objectives, the threat landscape, resources (including personnel), and constraints.'

OPM's Cybersecurity and Privacy Policy (p. 6-7) defines OPM's cybersecurity and privacy strategic objectives and requires alignment with NIST (p. 8). The OPM Risk management Framework (RMF) Implementation Procedures and Guidelines (IP&G) and OPM's Program Management (PM) IP&G define the process for developing Cybersecurity Profiles (p. 9 and pp. 8-9, respectively). Finally, OPM developed a Cybersecurity Profile document. Each of these documents and references were provided as requested during the audit. Additionally, the new OPM Director signed the re-establishment of OPM's Enterprise Risk Management (ERM) council. Also provided to the IG as a post-assessment artifact."

OIG Comment

This finding is related to the lack of policies and procedures that provide guidance for the development and maintenance of OPM's cybersecurity profiles. We received OPM's Cybersecurity and Privacy Policy, OPM Risk management Framework Implementation Procedures and Guidelines, and OPM's Program Management Implementation Procedures and Guidelines. These documents establish that profiles are maintained, however they do not contain all of the necessary elements including guidance related to the organization's mission objectives, threat landscape, resources (including personnel), and constraints.

As part of the audit resolution process, we recommend that OPM provide the Internal Oversight and Compliance Office with evidence that the agency implemented this recommendation.

Metric 2 – Cybersecurity Risk Management

FY 2025 Maturity Level: 2 – Defined. OPM has defined its risk management strategies that include the organization's priorities, constraints, risk tolerance and appetite statements, as well as assumptions. Additionally, OPM has established lines of communication for risks, including risks from suppliers and other third parties.

Further, OPM consistently implements its risk management strategies at the organizational, mission/business process, and system levels and calculates, documents, categorizes and prioritizes cybersecurity risks. However, OPM does not evaluate and adjust its cybersecurity risk management strategies based on its threat environment and risk assessments.

OPM does not evaluate and adjust its cybersecurity risk management strategies based on its threat environment and risk assessments.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Consistently Implemented*. We have assessed this metric as *Defined*. The recommendation below is to assist OPM with attaining the *Consistently Implemented* maturity level.

OMB M-16-17 requires compliance with OMB Circular A-123, which states that "The management of risk must be regularly reviewed to monitor whether or not the risk profile has changed and to gain assurance that risk management is effective or if further action is necessary. In addition, processes must be put in place to review whether risks still exist, whether new risks have arisen, whether the likelihood and impact of risks have changed, to report significant changes that adjust risk priorities, and deliver assurance on the effectiveness of control. In addition, the overall risk management process must be subjected to regular review to deliver assurance that it remains appropriate and effective. At a minimum, management's risk management review processes must: … ensure that all aspects of the risk management process are reviewed at least once a year; … ensure that risks themselves are subjected to review with appropriate frequency; and … make provisions for alerting the appropriate level of management to new or emerging risks, as well as changes in already identified risks, so that the change can be appropriately addressed."

Failure to adjust the risk management strategy to OPM's current risks increases the likelihood of a weakness or threat vector remaining or being improperly addressed in OPM's environment.

Recommendation 2

We recommend that OPM evaluate and adjust its cybersecurity risk management strategy based on its threat environment and organization-wide cyber and privacy risk assessment.

OPM Response

"Non-Concur. The draft NFR reads 'however, OPM did not submit evidence for evaluating and adjusting its risk management strategy based on its threat environment and risk assessment.'

OPM submitted its Fiscal Year (FY) 2025 Cybersecurity Program Plan, which defines its FY 2025 risk management strategy. This program plan was updated from the FY 2024 Cybersecurity Program Plan (which the IG also received) based on threat intelligence and information gained from risk assessment[s]."

OIG Comment

We received the FY 2025 Cybersecurity Program Plan that defines OPM's policy. However, this recommendation is to help OPM achieve the *Consistently Implemented* maturity level, which requires that OPM demonstrate a specific approach to evaluating and adjusting OPM's risk management strategy based on OPM's threat environment and risk assessment.

Metric 3 – Cybersecurity Roles

FY 2025 Maturity Level: 3 – Consistently Implemented. OPM has defined and communicated the structures of its team, as well as the roles and responsibilities of agency stakeholders within its Cybersecurity and Privacy Policy. OPM also ensures individuals are performing their respective roles by incorporating the tasks related to their responsibilities in agency workplans.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Consistently Implemented*. We have assessed this metric as *Consistently Implemented*.

Metric 4 – Cybersecurity Governance Additional Information

We have no additional comments regarding the Cybersecurity Governance program.

C. CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT

The Cybersecurity Supply Chain Risk Management (C-SCRM) domain focuses on OPM's systematic process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Cybersecurity Supply Chain Risk Management domain is "3 – *Consistently Implemented*."**

Metric 5 – Adherence to Cybersecurity and Supply Chain Requirements

FY 2025 Maturity Level: 3 – Consistently Implemented. OPM has developed and maintained a C-SCRM Strategy that defines OPM's C-SCRM requirements and processes, including acquisition and contractual security measures.

Additionally, OPM has consistently implemented its policies, procedures, and processes for assessing and reviewing the supply chain-related risks, including tools providing visibility into upstream suppliers and attestations of the controls within the contractor's/supplier's environment.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Consistently Implemented*. We have assessed this metric as *Consistently Implemented*.

Metric 6 – C-SCRM Additional Information

We have no additional comments regarding the C-SCRM program.

D. RISK AND ASSET MANAGEMENT

Risk and Asset Management metrics include OPM's established risk management program and asset management program. The Risk Management controls enable OPM to manage risk by establishing the context for risk-related activities, assessing risk, responding to risk once determined, and monitoring risk over time. The Asset Management controls enable OPM to identify and manage assets consistently with their relative importance to OPM's objectives and risk strategy. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Risk and Asset Management domain is "3 – Consistently Implemented."**

Metric 7 – Inventory of Major Systems and System Interconnections

FY 2025 Maturity Level: 4 – Managed and Measurable. OPM has defined policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information systems and system interconnections including the Enterprise Asset Management Plan.

Additionally, in accordance with the Enterprise Asset Management Plan, OPM has developed and maintained a comprehensive and accurate enterprise-wide inventory of systems and interconnections with necessary details for tracking, monitoring, and reporting, including the type of system (cloud, public-facing, third party); the controls that impact it; which program office it belongs to; and documentation of the hardware, software, and data involved with the system.

Further, as seen in the Weekly Cyber Metrics slide decks, OPM ensures that the inventoried information systems are subject to the monitoring processes defined within OPM's Information Security Continuous Monitoring (ISCM) strategy.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Managed and Measurable.* We have assessed this metric as *Managed and Measurable*.

Metric 8 – Hardware Inventory

FY 2025 Maturity Level: 3 – Consistently Implemented. OPM has defined policies, procedures, and processes for developing and maintaining an up-to-date inventory of hardware assets connected to OPM's network. OPM consistently reports 100% of its assets to the Department of Homeland Security's Continuous Diagnostics and Mitigation program which tracks hardware assets, software assets, security management configuration settings, and software vulnerabilities.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Consistently Implemented.* We have assessed this metric as *Consistently Implemented*.

Metric 9 – Software Inventory

FY 2025 Maturity Level: 1 – Ad Hoc. As part of the Enterprise Asset Management Plan, OPM is in the process of developing an enterprise software inventory list. However, due to the cancellation of the Enterprise Software Registry project, OPM has not finished documenting the processes and procedures for developing and maintaining the software inventory list.

OPM has not finished documenting the processes and procedures for developing and maintaining the Software Inventory/Registry.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Defined*. We have assessed this metric as *Ad Hoc*. The recommendation below is to assist OPM with attaining the *Defined* maturity level.

NIST SP 800-53, Revision 5, Control CM-1 states that organizations should "Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: … [Selection (one or more): Organization-level, Mission/business process-level, System-level] configuration management policy that: … Addresses purpose, scope, roles, responsibilities,

management commitment, coordination among organizational entities, and compliance; and … Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and … Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls; … ."

Additionally, NIST SP 800-53, Revision 5, Control CM-8 states that organizations should "Develop and document an inventory of system components that: … Accurately reflects the system; … Includes all components within the system; … Does not include duplicate accounting of components or components assigned to any other system; … Is at the level of granularity deemed necessary for tracking and reporting; and … Includes the following information to achieve system component accountability: [Assignment: organization-defined information]; and … Review and update the system component inventory [Assignment: organization-defined frequency]." Per the supplemental guidance for CM-8 and OPM's "Implementation Procedures and Guidelines: Configuration Management," software is a system component.

Failure to have policies and procedures for developing and maintaining a software inventory increases the likelihood that software is mismanaged and not secured.

Recommendation 3

We recommend that OPM develop policies and procedures for developing and maintaining software inventory.

OPM Response

"Concur. However, OPM does manually track all software inventory for the entire agency. That artifact will be provided to OIG."

OIG Comment

As part of the audit resolution process, we recommend that OPM provide the Internal Oversight and Compliance Office with evidence that the agency implemented this recommendation. This statement applies to all subsequent recommendations in this audit report that OPM agrees to implement.

Metric 10 – Data Inventory

FY 2025 Maturity Level: 1 – Ad Hoc. OPM is in the process of developing policies and procedures for maintaining a comprehensive and accurate inventory of data; however, it does not currently have the policies and procedures completed.

OPM has not provided any policies or procedures for developing and maintaining a data inventory.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Defined*. We have assessed this metric as *Ad Hoc*. The recommendation below is to assist OPM with attaining the *Defined* maturity level.

NIST SP 800-53, Revision 5, Control CM-1 states that organizations should "Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: … [Selection (one or more): Organization-level, Mission/business process-level, System-level] configuration management policy that: … Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and … Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and … Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls … ."

Additionally, NIST SP 800-53, Revision 5, Control CM-12 states that organizations should "Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored; … Identify and document the users who have access to the system and system components where the information is processed and stored; and Document changes to the location (i.e., system or system components) where the information is processed and stored."

NIST SP 800-53, Revision 5, Control CM-13 also states that organizations should "Develop and document a map of system data actions."

Failure to have policies and procedures for developing and maintaining a data inventory increases the likelihood that the data inventory is inaccurate and systems lack the security necessary for the data they store and process.

Recommendation 4

We recommend that OPM develop policies and procedures for developing and maintaining a data inventory.

OPM Response

"Concur. OPM OCIO has identified a path forward to develop policies and procedures, including the technology implementation to establish an operational process for maintaining our data inventory."

Metric 11 – Risk Policy and Strategy

FY 2025 Maturity Level: 4 – Managed and Measurable. OPM has defined its policies, procedures, and processes to manage cybersecurity risks associated with operating and maintaining its information systems through its Enterprise Risk Management Strategy and Process Guide, as well as the Cybersecurity Risk Management Strategy policy. Within the Security Authorization Guide, OPM has also ensured its policies, procedures, and processes cover cybersecurity risk management at the organizational, mission/business process, and information system levels.

Additionally, OPM has consistently implemented its policies, procedures, and processes to manage the cybersecurity risks associated with operating and maintaining its information systems through its Risk Assessment Reports and Assessment Results Tables for each system authorization package. OPM also employs a cybersecurity risk register to manage risks, as appropriate, and is consistently capturing and sharing lessons learned on the effectiveness of the cybersecurity risk program.

Further, OPM utilizes tools to consistently monitor the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level. Through the utilization of multiple tools and processes, OPM ensures the information in cybersecurity risk registers is obtained accurately, consistently, and in a reproducible format.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Managed and Measurable.* We have assessed this metric as *Managed and Measurable*.

Metric 12 – Centralized Enterprise-wide Risk Tool

FY 2025 Maturity Level: 4 – Managed and Measurable. Through the Plan of Action and Milestones (POA&M) guide and ISCM Strategy, OPM has identified and defined the requirements for an automated solution, which provides a centralized, enterprise-wide view of cybersecurity risks across the organization including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.

Additionally, OPM consistently implements an automated solution across the enterprise that provides a centralized, enterprise-wide view of risks across OPM including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards associated

with each system. OPM has also ensured all necessary sources of cybersecurity risk information are integrated into the solution.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Managed and Measurable.* We have assessed this metric as *Managed and Measurable*.

Metric 13 – Risk and Asset Management Other Information

We have no additional comments regarding the Risk Management program.

E. CONFIGURATION MANAGEMENT

Configuration Management controls allow an organization to establish information system configuration baselines, processes for securely managing changes to configurable settings, and procedures for monitoring system software. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Configuration Management domain is "2 – *Defined*."**

OPM has not established configuration settings/common secure configurations for all the systems in its environment.

Metric 14 –Configuration Settings/Common Secure Configurations

FY 2025 Maturity Level: 1 – Ad Hoc. OPM has developed policies and procedures for ensuring that configuration settings/common secure configurations are defined, implemented, and monitored for the majority of its systems. However, the agency has not established configuration settings/common secure configurations for two systems in its environment.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Consistently Implemented*. We have assessed this metric as *Ad Hoc*. The recommendation below is to assist OPM with attaining the Defined maturity level.

NIST SP 800-53, Revision 5, Control CM-6 states that an organization should "Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations] … ."

Failure to document the configuration settings prohibits OPM from monitoring compliance through its configuration baseline scanning procedures.

Recommendation 5

We recommend that OPM document the configuration settings/common secure configurations for all operating systems implemented within its environment.

OPM Response

"Concur."

Metric 15 –Flaw Remediation

FY 2025 Maturity Level: 2 – Defined. OPM has developed policies and procedures for flaw remediation. Policies and procedures include processes for identifying, validating, reporting, and rectifying information system flaws according to OPM's patching schedule. Additionally, procedures include processes for testing software updates in lower development environments and incorporating flaw remediation into the organization's configuration management protocols.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Defined*. We have assessed this metric as *Defined*.

Metric 16 – Configuration Management Other Information

We have no additional comments regarding the Configuration Management program.

F. IDENTITY AND ACCESS MANAGEMENT

The Identity and Access Management program is a government-wide effort to help federal agencies provision access to systems and facilities to the right person, at the right time, for the right reason. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Identity and Access Management domain is "3 – *Consistently Implemented*."**

Metric 17 – Multi-Factor Authentication

FY 2025 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented strong, multi-factor authentication mechanisms for non-privileged users of the organization's physical and logical assets, including remote access to networks. Additionally, public facing systems consistently utilize phishing resistant multi-factor authentication.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Consistently Implemented*. We have assessed this metric as *Consistently Implemented*.

Metric 18 – Strong Authentication Mechanisms for Privileged Users

FY 2025 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented strong, multi-factor authentication mechanisms for privileged users of the organization's physical and logical assets, and networks. This includes remote access to networks.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Consistently Implemented*. We have assessed this metric as *Consistently Implemented*.

Metric 19 – Management of Privileged User Accounts

FY 2025 Maturity Level: 3 – Consistently Implemented. OPM had defined and implemented its policies for provisioning, managing, and reviewing privileged accounts that include procedures logging, approval and tracking, and inventorying and validating. OPM also limits the functions that can be performed when using privileged accounts and limits the duration that privileged accounts can be utilized.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Consistently Implemented*. We have assessed this metric as *Consistently Implemented*.

Metric 20 – Identity and Access Management Other Information

We have no additional comments regarding the Identity and Access Management program.

G. DATA PROTECTION AND PRIVACY

The Data Protection and Privacy metrics address the controls related to the confidentiality, integrity, and availability of personally identifiable information and other agency sensitive data. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Data Protection and Privacy domain is "2 – Defined."**

Metric 21 – Data Protection and Privacy Policies and Procedures

FY 2025 Maturity Level: 2 – Defined. OPM has defined and communicated policies and procedures for encryption of data at rest, encryption of data in transit, removeable media, sanitizing digital media prior to disposal or reuse, and protecting data backups. Additionally, OPM has defined and communicated the expectations and controls for accessing personal communication applications, personal email, and external file sharing websites. However, OPM has three FISMA systems with encryption data in transit vulnerabilities. Although OPM has POA&Ms open to track the vulnerabilities, the milestones had estimated completion dates that have passed and have not subsequently been updated. Additionally, one FISMA system has had an open POA&M for encryption in transit vulnerabilities since FY 2022.

OPM has three FISMA systems with encryption data in transit vulnerabilities.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Consistently Implemented*. We have assessed this metric as *Defined*. The recommendation below is to assist OPM with attaining the *Consistently Implemented* maturity level.

OPM Implementation Procedures and Guidelines: System and Communications Protection states that OPM enforces encryption in transit at Open Systems Interconnection model layers four through seven to the maximum extent practicable.

NIST SP 800-53, Revision 5, control SC-8 states that an organization should "Protect the [Selection (one or more): confidentiality; integrity] of transmitted information."

Failure to remediate encryption vulnerabilities increases the risk that communication paths are exposed to the possibility of interception and modification.

Recommendation 6

We recommend that OPM remediate all data in transit vulnerabilities that the agency is currently tracking with POA&Ms.

OPM Response

"Concur. OPM needs to remediate PoAMs, but OPM has implemented EiT."

Metric 22 – Data Protection and Privacy Preventing Data Exfiltration

FY 2025 Maturity Level: 2 – Defined. OPM has developed policies and procedures for data exfiltration, endpoint detection and response, enhanced network defenses, email authentication, and Domain Name System tampering. However, we found that the policies and procedures have not been consistently implemented as it relates to its security logging capabilities. OPM is not capturing/ingesting logs into its security information and event management system for investigative purposes.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Managed and Measurable*. We have assessed this metric as *Defined*. The recommendation below is to assist OPM with attaining the C*onsistently Implemented* maturity level.

NIST SP 800-53, Revision 5, control SI-4 states that an organization should "Monitor the system to detect: … Attacks and indicators of potential attacks" to analyze detected events and anomalies."

In addition, OPM's Implementation Procedures and Guidelines: System and Information Integrity states that "bidirectional monitoring is essential for identifying such activities as lateral movement of malware, unauthorized communication channels, and event reconstruction in support of incident handling activities."

Failure to review security logs from FISMA systems increases the risk that incident response efforts are hindered.

Recommendation 7

We recommend that OPM ingest security logs from its FISMA systems and analyze events and anomalies.

OPM Response

"Non-Concur. OPM developed an agency-specific event log integration strategy to align with M-21-31, which includes multiple phases and associated timelines. This phased approach was approved by OPM leadership and is consistent with supplemental guidance issued by CISA. In alignment with its approved implementation strategy, OPM currently ingests event logs for the High Value Assets (HVA) systems and financial systems. OPM has developed a timeline for log ingestion for the rest of our FISMA systems to be completed prior to the end of FY26."

OIG Comment

OPM has multiple FISMA systems that have open POA&Ms for not capturing/ingesting logs into the security information and event management tool for investigative purposes. As stated in the response, "OPM has developed a timeline for log ingestion for the rest of our FISMA systems to be completed prior to the end of FY26." This demonstrates that OPM has not completed the process for log ingestion and continues to work towards this goal. A score of consistently implemented cannot be achieved until the agency consistently conducts the activity detailed in the metric.

Metric 23 – Data Protection and Privacy Other Information

We have no additional comments regarding the Data Protection and Privacy program.

H. SECURITY TRAINING

FISMA requires that all government employees and contractors take annual IT security awareness training. Employees with IT security responsibility are required to take specialized training specific to their job function. **OPM's overall maturity level for the Security Training domain is "*2 – Defined*."**

Metric 24 – Assessment of Workforce

FY 2025 Maturity Level: 2 – Defined. OPM has defined its process for assessing the knowledge, skills, and abilities of its workforce to determine its specialized training needs and periodically updating its assessment to account for a changing risk environment. Further, the organization has also assessed the knowledge, skills, and abilities of its workforce and has identified skills gaps.

OPM has not utilized the results of its workforce assessment and skills gap analysis to update its awareness and training strategies or plans.

However, OPM has not utilized the results of its workforce assessment and skills gap analysis to update its awareness and training strategies or plans required by OPM's Implementation Procedures and Guidelines: Awareness and Training policy.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Consistently Implemented*. We have assessed this metric as *Defined*. The recommendation below is to assist OPM with attaining the *Consistently Implemented* maturity level.

NIST SP 800-53, Revision 5, Control AT-2 c. states that the organization should "Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] … ."

NIST SP 800-53, Revision 5, Control AT-3 b. states that the organization should "Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events] … ."

OPM's OCIO Implementation Procedures and Guidelines: Awareness and Training, dated May 31, 2024, states that "Quantitative and qualitative analysis of gap analysis will be used to inform the effectiveness of the training and awareness program and to update the training material to address identified deficiencies."

Failure to update security and privacy awareness, literacy, and role-based training can have significant negative impacts on OPM's risk posture, compliance, and operational resilience.

Recommendation 8

We recommend that OPM update its literacy, awareness and role-based training content using the results from workforce assessments and skills gap analysis.

OPM Response

"Concur."

Metric 25 – Security Training Other Information

We have no additional comments regarding Security Training program.

I. INFORMATION SECURITY CONTINUOUS MONITORING

ISCM metrics address the controls related to performing ongoing information system assessments. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Information Systems Continuous Monitoring domain is "2 – Defined."**

Metric 26 – ISCM Strategies and Policies

FY 2025 Maturity Level: 2 – Defined. OPM has defined and communicated a system level continuous monitoring strategy that defines its processes for performing ongoing security control assessments and monitoring activities. Additionally, OPM has also developed a Security Authorization Guide that defines its processes for granting system authorizations, maintaining system security plans, and time-based triggers for ongoing authorizations.

OPM has 35 systems that have over 740 IT security controls that are partially or are not satisfied, whereas only 208 POA&Ms are open to monitor risks.

OPM's continuous monitoring strategy addresses security control monitoring at the organization and business units. However, ISCM testing performed by OPM revealed 35 systems have over 740 IT security controls that are partially or are not satisfied, whereas only 208 POA&Ms are open to monitor risks. Therefore, OPM has not consistently documented POA&Ms for risks it has identified during ISCM activities. Additionally, it was unable to sufficiently demonstrate that it consistently captures lessons learned to make improvements to the ISCM strategy.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Managed and Measurable*. We have assessed this metric as *Defined*. The recommendations below are to assist OPM with attaining the C*onsistently Implemented* maturity level.

NIST SP 800-37, Revision 2, states that an organization "Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in places of action and milestones." The OPM POA&M Guide states that "Similar to security authorizations, ongoing security control assessments may uncover weaknesses in a system. Test results from the

Information Security Continuous Monitoring (ISCM) report are used to populate the weakness description in the POA&M."

NIST SP 800-37, Revision 2, states that "Incorporating lessons learned facilitates the consistent progression of the continuous monitoring and ongoing authorization implementation from the lowest to the highest impact levels for the system within the organization."

Failure to document weaknesses identified during ISCM activities increases the likelihood that appropriate risk response actions are not taken. In addition, failure to consistently capture lessons learned increases the risk that improvements to the ISCM strategy/policies are delayed.

Recommendation 9

We recommend that OPM document POA&Ms for all ISCM risks.

OPM Response

"Concur. However, from lessons learned OPM has updated the PoAM process (2025) for tracking and closing only the significant findings to reduce paperwork and manhours."

Recommendation 10

We recommend that OPM document lessons learned to improve its ISCM policies and strategy.

OPM Response

"Concur. However, much of OPM's 2025 updates have all come from lessons learned to drive automation and reduce paperwork. Going forward, OPM will document the lessons learned in a document for the OIG to review."

Metric 27 – ISCM Measuring Integrity and Security Posture

FY 2025 Maturity Level: 2 – Defined. OPM has defined policies and procedures to monitor and measure the security posture of its assets. The OPM ISCM Implementation Strategy defines roles and responsibilities, ongoing security control assessments, reporting, response, and system software development life cycle. Further, the Cybersecurity and Privacy policy establishes and defines ISCM roles for the Senior Agency Official for Privacy, Chief Information Security Officer, System Owner, and Information System Security Officer.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Defined*. We have assessed this metric as *Defined*.

Metric 28 – ISCM Ongoing Security Assessments

FY 2025 Maturity Level: 2 – Defined. OPM has defined and communicated a system level continuous monitoring strategy that describes its processes for performing ongoing security control assessments and monitoring activities.

In response to an information request, OPM stated that its cloud systems follow the FedRAMP ISCM program. However, OPM ISCM policies or procedures do not address how cloud inherited controls are monitored, or how changes to cloud systems are monitored and reported through ISCM activities.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Managed and Measurable*. We have assessed this metric as *Defined*. The recommendation below is to assist OPM with attaining the *Consistently Implemented* maturity level.

NIST SP 800-137, states that "ISCM strategies and programs are not static. Security control assessments, security status metrics and monitoring and assessment frequencies change in accordance with the needs of the organization. The continuous monitoring strategy is reviewed to ensure that it sufficiently supports the organization in operating within acceptable risk tolerance levels, that metrics remain current and complete. The strategy review also identifies ways to improve organizational insight into security posture, effectively supports informed risk management decision making/ongoing authorizations, and improves the organization's ability to respond to known and emerging threats."

Failure to monitor cloud service provider(s) for weakness increases the likelihood that the agency is unaware of risks to its security posture.

Recommendation 11

We recommend that OPM update its ISCM strategies to include policies and procedures to monitor its cloud service providers security posture.

OPM Response

"Concur."

Metric 29 – ISCM Other Information

We have no additional comments regarding the ISCM program.

J. INCIDENT RESPONSE

Incident response or incident handling controls assist OPM in preparing for, detecting, analyzing, containing, eradicating, recovering from, and learning lessons from incidents. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Incident Response domain is "3 – *Consistently Implemented*."**

Metric 30 – Incident Detection and Analysis

FY 2025 Maturity Level: 2 – Defined. OPM has defined policies, procedures, and processes for incident detection, analysis, and prioritization. OPM has also utilized its Incident Response Plan and Playbooks for specific types of incidents while investigating and resolving security events.

OPM has approximately 19 systems that do not meet EL1 logging requirements.

Additionally, OPM consistently captures and shares lessons learned on the effectiveness of its incident detection policies and procedures and making updates as necessary.

We examined 55 FISMA systems that should be at a minimum of Event Logging (EL) Tier 1 (Basic), which requires an organization to meet logging requirements of highest criticality including logging categories, a time standard, and basic centralized access. However, 19 systems do not meet EL1 logging requirements.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Optimized*. We have assessed this metric as *Defined*. The recommendation below is to assist OPM with attaining the *Consistently Implemented* maturity level.

OMB Memorandum M-21-31 states that, within one year of August 27, 2021, agencies should "reach EL1 maturity." EL1 maturity includes but is not limited to ensuring event logs contain specific data (if applicable), basic centralized access is implemented, and planning for implementation of User Behavior Monitoring and Security, Orchestration, Automation, and Response (SOAR) capabilities is completed.

Failure to implement logging increases the likelihood that incidents remain undetected or result in improper analysis.

Recommendation 12

We recommend that OPM configure the agency logs/logging tools to meet the EL1 (basic) logging requirements outlined in M-21-31.

OPM Response

"Non-concur: OPM feels that this is a duplicate recommendation from #7 above and the OPM should not be penalized twice for the same issue. Our response to this recommendation is the same as recommendation #7."

OIG Comment

The basis for this finding is related to EL1 logging requirements such as time standard, event forwarding, passive domain name system, etc. as mentioned in OMB Memorandum M-21-31. Metric 22 and the associated recommendation is related to capturing/ingesting logs into a security information and event management system for investigative purposes. Therefore, each metric has different requirements.

Metric 31 – Incident Handling

FY 2025 Maturity Level: 4 – Managed and Measurable. Within OPM's Incident Response Playbooks, OPM has defined its policies, procedures, and processes for incident handling to include containment, eradication, mitigation, and recovery strategies for each key incident type.

Additionally, OPM has consistently implemented these playbooks when conducting tabletop exercises and responding to incidents. OPM has also consistently captured and protected incident data and metadata at the enterprise-wide level through its incident response tools.

Further, OPM monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident handling policies and procedures. OPM also ensures that the data supporting the metrics is obtained accurately, consistently, and in a reproducible format.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Managed and Measurable*. We have assessed this metric as *Managed and Measurable*.

Metric 32 – Incident Response Other Information

We have no additional comments regarding the Incident Response program.

K. CONTINGENCY PLANNING

Contingency planning includes the policies and procedures that ensure adequate availability of information systems, data, and business processes. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Contingency Planning domain is "3 – *Consistently Implemented*."**

Metric 33 – Business Impact Analysis

FY 2025 Maturity Level: 3 – Consistently Implemented. OPM has defined its policies, procedures, and processes for conducting organizational and system-level business impact analysis. OPM has also consistently incorporated the results of organizational and system level business impact analysis into strategy and contingency plan development efforts.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Consistently Implemented*. We have assessed this metric as *Consistently Implemented*.

Metric 34 – Contingency Plan Testing

FY 2025 Maturity Level: 2 – Defined. OPM has defined its policies, procedures, and processes for information system contingency plan (ISCP) testing and exercises.

Six ISCP tests have exceeded the annual update.

Additionally, OPM has implemented and conducted routine ISCP testing to ensure that critical systems can be recovered within established timeframes after a disruption or disaster.

However, our testing found that six ISCP tests have exceeded the annual update deadlines. Two of those six are high value asset systems.

In the self-assessment OPM conducted, the maturity level goal for this metric was *Consistently Implemented*. We have assessed this metric as *Defined*. The recommendation below is to assist OPM with attaining the *Consistently Implemented* maturity level.

NIST SP 800-53, Revision 5, Control CP-4 states that the organization should "Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests]."

OPM's OCIO, Implementation and Procedures and Guidelines, Contingency Planning policy states that all ISCPs must be tested annually.

Failure to consistently implement ISCP testing could lead to OPM's inability to recover a critical system in the event of a crisis. If an incident were to occur, untested ISCPs may be ineffective or unusable, leading to delayed recovery.

Recommendation 13

We recommend that OPM test all ISCP's annually as required by OPM policy.

OPM Response:

"Concur."

Metric 35 – Contingency Planning Other Information

We have no additional comments regarding the ISCP program.

APPENDIX I – Detailed FISMA Results by Metric

1 – Ad Hoc **2 – Defined** **3 – Consistently Implemented** **4 – Managed and Measurable** **5 - Optimized**

Function	Metric	Metric Name	Metric Maturity Level	Function Score	New Recommendation
Govern		**Cybersecurity Governance**	**2.00**		
Govern	1	Cybersecurity Profiles	1		1
Govern	2	Cybersecurity Risk Management	2		1
Govern	3	Cybersecurity Roles	3		0
Govern	4	Cybersecurity Governance Additional Information	N/A		0
Govern		**Cybersecurity Supply Chain Risk Management (C-SCRM)**	**3**		
Govern	5	Adherence to Cybersecurity and Supply Chain Requirements	3		0
Govern	6	C-SCRM Additional Information	N/A		
Govern		**OVERALL GOVERN SCORE**		**2.5**	
Identify		**Risk and Asset Management**	**2.83**		
Identify	7	Inventory of Major Systems and System Interconnections	4		0
Identify	8	Hardware Inventory	3		0
Identify	9	Software Inventory	1		1
Identify	10	Data Inventory	1		1
Identify	11	Risk Policy and Strategy	4		0
Identify	12	Centralized Enterprise-wide Risk Tool	4		0
Identify	13	Risk and Asset Management Other Information	N/A		
Identify		**OVERALL IDENTIFY SCORE**		**2.83**	0
Protect		**Configuration Management**	**1.50**		
Protect	14	Configuration Settings/Common Secure Configurations	1		1
Protect	15	Flaw Remediation	2		0
Protect	16	Configuration Management Other Information	N/A		0
Protect		**Identity and Access Management**	**3.00**		
Protect	17	Multi-Factor Authentication	3		0
Protect	18	Strong Authentication Mechanisms for Privileged Users	3		0
Protect	19	Management of Privileged User Accounts	3		0
Protect	20	Identity and Access Management Other Information	N/A		0

Function	Metric	Metric Name	Metric Maturity Level	Function Score	New Recommendation
Protect		**Data Protection and Privacy**	**2**		
Protect	21	Data Protection and Privacy Policies and Procedures	2		1
Protect	22	Data Protection and Privacy Preventing Data Exfiltration	2		1
Protect	23	Data Protection and Privacy Other Information	N/A		0
Protect		**Security Training**	**2**		
Protect	24	Assessment of Workforce	2		1
Protect	25	Security Training Other Information	N/A		0
Protect		**OVERALL PROTECT SCORE**		**2.125**	
Detect		**Information Security Continuous Monitoring (ISCM)**	**2.00**		
Detect	26	ISCM Strategies and Policies	2		2
Detect	27	ISCM Measuring Integrity and Security Posture	2		0
Detect	28	ISCM Ongoing Security Assessments	2		1
Detect	29	ISCM Other Information	N/A		0
Detect		**OVERALL DETECT SCORE**	N/A	**2**	0
Respond		**Incident Response**	**3.00**		
Respond	30	Incident Detection and Analysis	2		1
Respond	31	Incident Handling	4		0
Respond	32	Incident Response Other Information	N/A		0
Respond		**OVERALL RESPOND SCORE**		**3**	
Recover		**Contingency Planning**	**2.50**		
Recover	33	Business Impact Analysis	3		0
Recover	34	Contingency Plan Testing	2		1
Recover	35	Contingency Planning Other Information	N/A		0
Recover		**OVERALL RECOVER SCORE**		**2.5**	
		OVERALL MATURITY & TOTAL RECOMENDATIONS		**2.49**	**13**

APPENDIX II – Status of Prior OIG Audit Recommendations

The table below outlines the status of recommendations issued in the FY 2024 FISMA audit (Report No.2024-ISAG-008).			
Rec #	**Recommendation**	**Recommendation History**	**Current Status**
1	We recommend that OPM integrate its configuration management plan into the risk management and continuous monitoring programs, and utilize lessons learned to make improvements to the plan.	Rolled Forward from 2023	CLOSED 3/21/25
2	We recommend that OESPIM develop a SORN for all applicable systems.	New in 2024	OPEN
3	We recommend that OPM develop and conduct an updated assessment of its workforce's knowledge, skills, and abilities to identify any skill gaps and specialized training needs.	Rolled Forward from 2023	CLOSED 2/6/25
4	We recommend that OPM obtain feedback on its security awareness and training program and use the information to make improvements to the IT security training program.	New in 2024	OPEN

APPENDIX III

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Chief Information
Officer

September 18, 2025

MEMORANDUM FOR: Eric Keehan
Chief, Information Systems Audit Group
Office of the Inspector General

FROM: Perryn Ashmore
Acting Chief Information Officer

SUBJECT: Management Response to the Office of the Inspector General Federal Information Security Modernization Act Audit – FY 2025 (Report No. 2025-ISAG-008)

The Office of the Chief Information Officer (CIO) appreciates the opportunity to provide comments to the Office of the Inspector General (OIG) draft report, the Federal Information Security Modernization Act (FISMA) Fiscal Year 2025, Report No. 2025-ISAG-008. We thank the Office of Inspector General's (OIG) cooperation, open dialogue, and partnership in our effort to safeguard our customer's data and the systems that process that data. Our itemized responses to the FY 2025 recommendations are below.

Recommendation 1: We recommend OPM update the Enterprise Risk Management Strategy and Process Guide to accurately reflect the development and maintenance of OPM's cybersecurity profiles.

Management Response: Non-Concur. The draft NFR reads "however, OPM lacked supporting documentation for the development and maintenance of the current and target profiles that includes OPM's mission objectives, the threat landscape, resources (including personnel), and constraints."

OPM's Cybersecurity and Privacy Policy (p. 6-7) defines OPM's cybersecurity and privacy strategic objectives and requires alignment with NIST (p. 8). The OPM Risk management Framework (RMF) Implementation Procedures and Guidelines (IP&G) and OPM's Program

Management (PM) IP&G define the process for developing Cybersecurity Profiles (p. 9 and pp. 8-9, respectively). Finally, OPM developed a Cybersecurity Profile document. Each of these documents and references were provided as requested during the audit. Additionally, the new OPM Director signed the re-establishment of OPM's Enterprise Risk Management (ERM) council. Also provided to the IG as a post-assessment artifact.

Recommendation 2: We recommend OPM evaluate and adjust its cybersecurity risk management strategy based on its threat environment and organization wide cyber and privacy risk assessment.

Management Response: Non-Concur. The draft NFR reads "however, OPM did not submit evidence for evaluating and adjusting its risk management strategy based on its threat environment and risk assessment."

OPM submitted its Fiscal Year (FY) 2025 Cybersecurity Program Plan, which defines its FY 2025 risk management strategy. This program plan was updated from the FY 2024 Cybersecurity Program Plan (which the IG also received) based on threat intelligence and information gained from risk assessments.

Recommendation 3: We recommend that OPM develop policies and procedures for developing and maintaining software inventory.

Management Response: Concur. However, OPM does manually track all software inventory for the entire agency. That artifact will be provided to OIG.

Recommendation 4: We recommend that OPM develop policies and procedures for developing and maintaining a data inventory.

Management Response: Concur. OPM OCIO has identified a path forward to develop policies and procedures, including the technology implementation to establish an operational process for maintaining our data inventory.

Recommendation 5: We recommend that OPM document the settings/common secure configurations for all operating systems implemented within its environment

Management Response: Concur.

Recommendation 6: We recommend that OPM remediate all data in transit vulnerabilities that the agency is currently tracking with POA&Ms.

Management Response: Concur. OPM needs to remediate PoAMs, but OPM has implemented EiT.

Recommendation 7: We recommend that OPM ingest security logs from its FISMA systems and analyze events and anomalies.

Management Response: Non-Concur. OPM developed an agency-specific event log integration strategy to align with M-21-31, which includes multiple phases and associated timelines. This phased approach was approved by OPM leadership and is consistent with supplemental guidance issued by CISA. In alignment with its approved implementation strategy, OPM currently ingests event logs for the High Value Assets (HVA) systems and financial systems. OPM has developed a timeline for log ingestion for the rest of our FISMA systems to be completed prior to the end of FY26.

Recommendation 8: We recommend that OPM update its literacy, awareness and role-based training content using the results from workforce assessments and skills gap analyses.

Management Response: Concur.

Recommendation 9: We recommend that OPM document POA&Ms for all ISCM risks.

Management Response: Concur. However, from lessons learned OPM has updated the PoAM process (2025) for tracking and closing only the significant findings to reduce paperwork and manhours.

Recommendation 10: We recommend that OPM document lessons learned to improve its ISCM policies and strategy.

Management Response: Concur. However, much of OPM's 2025 updates have all come from lessons learned to drive automation and reduce paperwork. Going forward, OPM will document the lessons learned in a document for the OIG to review.

Recommendation 11: We recommend that OPM update its ISCM strategies to include policies and procedures to monitor its cloud service providers security posture.

Management Response: Concur.

Recommendation 12: We recommend that OPM configure the agency logs/logging tools to meet the EL1 (basic) logging requirements outlined in M-21-31.

Management Response Non-concur: OPM feels that this is a duplicate recommendation from #7 above and the OPM should not be penalized twice for the same issue. Our response to this recommendation is the same as recommendation #7.

Recommendation 13: We recommend that OPM test all ISCP's annually as required by OPM policy.

Management Response: Concur.

cc:
Larry Allen
Associate Chief Information Officer
Danielle Rowell
Chief Information Security Officer

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: https://oig.opm.gov

By Phone: Toll Free Number: (877) 499-7295

By Mail: Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100

Report No. 2025-ISAG-008