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 2026

Report Number 2026-ISAG-003
November 4, 2026

EXECUTIVE SUMMARY

Federal Information Security Modernization Act Audit - Fiscal Year 2026

Report No. 2026-ISAG-003 **November 4, 2026**

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 Fiscal Year 2025 Inspector General (IG) FISMA Reporting Metrics. The previously approved U.S. Office of Management and Budget Fiscal Year 2025 Inspector General FISMA Reporting Metrics remained in effect for the fiscal year 2026 reporting period and served as the applicable criteria for this audit.

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 the Fiscal Year 2025 IG FISMA Reporting Metrics. Our audit was conducted from December 2025 through July 2026 at OPM headquarters in Washington, D.C.



Larry R. Price Jr.
Assistant Inspector General for Audits

What Did We Find?

The FISMA Inspector General reporting metrics use a maturity model evaluation system derived from the National Institute of Standards and Technology's (NIST) Cybersecurity Framework. The Cybersecurity Framework is comprised of 10 domain areas, and the averages of the domain scores are used to derive the agency's overall cybersecurity score. In fiscal year 2026, OPM's cybersecurity maturity level is measured as "3 – Consistently Implemented."

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 has defined policies and procedures for developing and maintaining its current and target cybersecurity profiles. OPM's documentation demonstrates consideration for OPM's mission objectives, threat landscape, resources (including personnel), and constraints. OPM has also defined its risk management strategies that include the organization's priorities, constraints, risk tolerance, and appetite statements as well as assumptions.

Cybersecurity Supply Chain Risk Management – 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 or supplier's environment.

Risk and Asset Management – OPM has developed and maintains a comprehensive enterprise-wide inventory of systems and interconnections with necessary details for tracking, monitoring, and reporting. However, within the FISMA system inventory, there are multiple systems that state there are no interconnections while listing interconnections in other fields.

Configuration Management – OPM has documented and maintains security configuration baselines for all operating platforms. OPM asserts that exceptions or deviations from the baseline configurations are managed through its risk management and system authorization process. OPM's Implementation Procedures and Guidelines: Risk Management Framework states that any operational obstacles, such as deviations, can be identified during the control implementation step. However, Security Content Automation Protocol–based compliance scans of Windows Server hosts revealed multiple compliance check failures against the applicable baseline.

Identity and Access Management – OPM has defined and implemented strong multifactor 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 multifactor authentication. While the process for conducting the digital identity risk assessments relies on a withdrawn NIST publication, OPM is within the timeframe defined by U.S. Office of Management and Budget (OMB) Circular A-130 to update the process.

Data Protection and Privacy – OPM participates in the Cybersecurity and Infrastructure Security Agency's (CISA) Continuous Diagnostics and Mitigation Program to strengthen its cybersecurity posture, and it uses CISA's Protective Domain Name System for all external Domain Name System queries. OPM also asserted that its risk management framework procedures require applicable systems and services to undergo penetration tests. However, OPM submitted only a data loss prevention test dated 2023. Despite our request for more recent results, as of the date of this report, OPM did not provide clarification, updated test results within the scope of this audit, or penetration test results demonstrating that it conducts routine exfiltration exercises.

Security Training – OPM has defined its process for assessing the knowledge, skills, and abilities of its workforce to determine its specialized training needs. It periodically updates its assessment to account for a changing risk environment. Further, OPM has conducted a skills gap analysis to assess and identify gaps in the knowledge, skills, and abilities of its workforce related to 92 competencies. OPM identified critical competency gaps that should be prioritized and developed action plans to address the gaps.

Information Security Continuous Monitoring – OPM developed and communicated a new Information System Continuous Monitoring Implementation Plan. The plan establishes monitoring requirements at each organizational tier, defines minimum monitoring frequencies, and describes an approach for ongoing control assessments. Under this approach, OPM is to annually select a subset of controls from the applicable NIST Special Publication 800-53B baseline and document the controls in an annual assessment plan. OPM subsequently provided an annual assessment plan covering its FISMA systems; however, it did not provide evidence that it conducted the assessments identified in the plan.

Incident Response – 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. However, an assessment was completed that indicated eight systems are still being onboarded, and four High Value Assets still have coverage gaps. Additionally, all 51 systems still need a system-level assessment to verify their onboarding status. These gaps demonstrate OPM is not capturing and protecting all incident data and metadata at an enterprise-wide level.

Contingency Planning – OPM has defined its policies, procedures, and processes for conducting organizational and system-level business impact analyses (BIAs) and for incorporating the results into strategy and plan development efforts, such as information system contingency plans (ISCPs). However, our testing found that OPM did not incorporate the recovery metrics from 15 system-level BIAs into the ISCPs.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
BIA	**Business Impact Analysis**
CIGIE	**Council of the Inspectors General on Integrity and Efficiency**
CISA	**Cybersecurity and Infrastructure Security Agency**
C-SCRM	**Cybersecurity Supply Chain Risk Management**
DHS	**U.S. Department of Homeland Security**
DNS	**Domain Name System**
FISMA	**Federal Information Security Modernization Act**
FY	**Fiscal Year**
IG	**Inspector General**
ISCM	**Information Security Continuous Monitoring**
ISCP	**Information System Contingency Plan**
IT	**Information Technology**
MFA	**Multifactor Authentication**
NIST	**National Institute of Standards and Technology**
OCIO	**Office of the Chief Information Officer**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
SP	**Special Publication**

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

ABBREVIATIONS iv

I. **BACKGROUND** 1

II. **OBJECTIVE, SCOPE, AND METHODOLOGY** 2

III. **AUDIT FINDINGS AND RECOMMENDATIONS** 5

A. Introduction and Overall Assessment 5

B. Cybersecurity Governance 7

C. Cybersecurity Supply Chain Risk Management 8

D. Risk and Asset Management 9

E. Configuration Management 13

F. Identity and Access Management 15

G. Data Protection and Privacy 16

H. Security Training 17

I. Information Security Continuous Monitoring 19

J. Incident Response 20

K. Contingency Planning 22

APPENDIX I: Detailed FISMA Results by Metric

APPENDIX II: Status of Prior OIG Audit Recommendations

APPENDIX III: The Office of Personnel Management's October 2, 2026, response to the draft audit report issued September 25, 2026

REPORT FRAUD, WASTE, AND MISMANAGEMENT

I. BACKGROUND

The 2002 Federal Information Security Management Act requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the U.S. Office of Management and Budget (OMB) on the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. The 2014 Federal Information Security Modernization Act (FISMA) reemphasizes the need for an annual IG evaluation. In accordance with FISMA, we conducted an audit of the U.S. Office of Personnel Management's (OPM) 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 agencywide 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 IGs in fulfilling their FISMA evaluation and reporting responsibilities, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in coordination with OMB, the U.S. Department of Homeland Security (DHS), and the Federal Chief Information Officers and Chief Information Security Officers councils, issued the Fiscal Year 2025 Inspector General FISMA Reporting Metrics. This document provides a methodology and format for agencies to report FISMA audit results to OMB. It identifies a series of reporting topics that relate to specific agency responsibilities outlined in FISMA. The previously approved OMB Fiscal Year 2025 Inspector General FISMA Reporting Metrics remained in effect for the fiscal year (FY) 2026 reporting period and served as the applicable criteria for this audit.

CIGIE, 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 the 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.

It should be noted that we also performed and issued a separate IT controls audit report focused on one of OPM's major information systems: Freedom of Information Act 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 FY 2026.

As in prior years, we requested that OPM conduct a self-assessment. This self-assessment gave the agency the opportunity to document its current maturity level for each metric and the maturity level it hoped to achieve by the end of FY 2027. We validated OPM's stated/current maturity level throughout FY 2026 and reported on the results of our analysis. We made

recommendations 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 OMB'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 the inspection of various documents, including IT and other related organizational policies and procedures. We used this understanding to evaluate the degree to which OPM designed and implemented the appropriate internal controls. 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 samples 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, based on available information, we concluded 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;
- NIST SP 800-53B, Control Baselines for Information Systems and Organizations;
- NIST CSF ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained;
- 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;
- OMB Circular A-130;
- OPM Information Technology Security FISMA Procedures;
- Public Law 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 2025 through July 2026 in OPM's Washington, D.C. office.

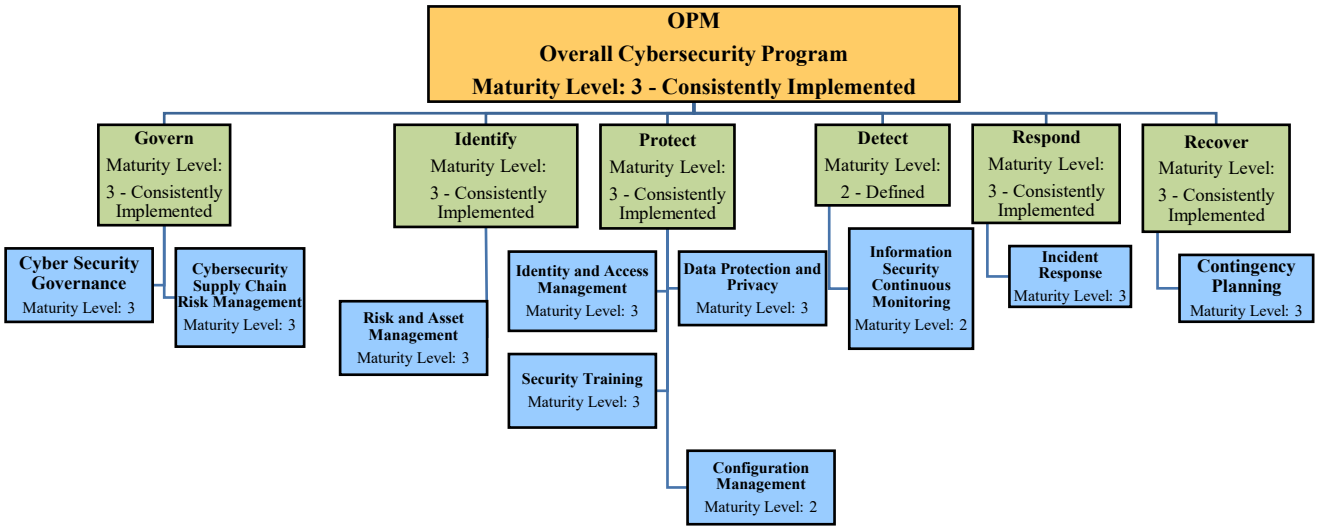
COMPLIANCE WITH LAWS AND REGULATIONS

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 five function areas that mapped to the nine domains under the function areas. In FY 2026, the Cybersecurity Framework is comprised of 6 function areas that map to the 10 domains under each function area. These 10 domains are broad cybersecurity 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 from 1 to 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.

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 changes.
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 landscape and business/mission needs.

There are core and supplemental scores for each function area. There was a focus on a calculated average approach—wherein the average of the metrics in a particular domain and the average between the core and supplemental scores will be used to determine the effectiveness of function areas (*govern*, *identify*, *protect*, *detect*, *respond*, and *recover*)—and the overall program.

Function	Core	FY 2026 Supplemental	FY 2026 Calculated Average	FY 2026 Assessed Maturity
Govern	3.00	3.00	3.00	Consistently Implemented (Level 3)
Identify	3.00	2.00	2.50	Consistently Implemented (Level 3)
Protect	2.75	N/A	2.75	Consistently Implemented (Level 3)
Detect	2.00	2.00	2.00	Defined (Level 2)
Respond	2.50	N/A	2.50	Consistently Implemented (Level 3)
Recover	2.50	N/A	2.50	Consistently Implemented (Level 3)
Overall Maturity	**2.63**	**2.33**	-	**Consistently Implemented (Level 3)***

*For the overall maturity level, we placed greater emphasis on the core metrics because they are assessed annually and represent a combination of Administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness. With a score of 2.63, these metrics surpass the threshold of 2.5 required to be deemed effective. As a result, the overall maturity is considered effective.

The remaining sections of this report provide the detailed results of our audit. Sections B through K 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.

OPM's overall maturity level for the Cybersecurity Governance domain is "3 – *Consistently Implemented*."

The sections below detail the results for each individual metric in this domain.

Metric 1 – Cybersecurity Profiles

FY 2026 Maturity Level: 3 – Consistently Implemented. OPM has defined policies and procedures for developing and maintaining its current and target cybersecurity profiles. OPM's documentation demonstrates consideration for OPM's mission objectives, threat landscape, resources (including personnel), and constraints. OPM has developed and maintained its current and target cybersecurity profiles, which describe OPM's current cybersecurity status and goals.

OPM has developed and maintained its cybersecurity profiles.

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 2 – Cybersecurity Risk Management

FY 2026 Maturity Level: 3 – Consistently Implemented. 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 cybersecurity risks, such as reports, plans of action and milestones, and emails that detail risks from internal and external sources (e.g., suppliers and other third parties).

Further, OPM consistently implements its risk management strategies at the organizational, mission/business process, and system levels, and it calculates, documents, categorizes, and prioritizes cybersecurity risks. Additionally, OPM evaluates and adjusts 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 *Consistently Implemented*.

Metric 3 – Cybersecurity Roles

FY 2026 Maturity Level: 3 – Consistently Implemented. OPM has defined and communicated the structure of its teams (e.g., system teams and the Risk Management Council) that include the roles and responsibilities of stakeholders and their levels of authority and dependencies. OPM also ensures individuals are performing their respective roles by incorporating the tasks related to their responsibilities into role-based performance metrics.

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.

OPM's overall maturity level for the Cybersecurity Supply Chain Risk Management domain is "3 – *Consistently Implemented*."

The sections below detail the results for the metric in this domain.

Metric 5 – Adherence to Cybersecurity and Supply Chain Requirements

FY 2026 Maturity Level: 3 – Consistently Implemented. OPM has developed and maintains a C-SCRM strategy that defines OPM's C-SCRM requirements and processes, including acquisition and contractual security measures.

OPM has implemented its policies for reviewing their supply chain-related risks.

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 or 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 address 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.

OPM's overall maturity level for the Risk and Asset Management domain is "3 – *Consistently Implemented*."

The sections below detail the results for each individual metric in this domain.

Metric 7 – Inventory of Major Systems and System Interconnections

FY 2026 Maturity Level: 2 – Defined. OPM has defined policies, procedures, and processes for developing and maintaining a comprehensive and accurate inventory of its information systems and system interconnections.

There are multiple systems that state there are no interconnections while listing interconnections in the other fields.

Additionally, in accordance with the Cybersecurity and Privacy Policy, OPM has developed and maintains a comprehensive 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 Implementation Plan: Information System Continuous Monitoring.

However, several systems in the FISMA system inventory are recorded as having no interconnections even though other fields list interconnections. Additionally, the authorization packages within OPM's governance, risk, and compliance tool, Archer, have several systems that state in the "Public Facing?" field that there are no public-facing components while listing public-facing URLs in other fields.

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 following recommendation is to assist OPM with attaining the *Consistently Implemented* maturity level.

NIST CSF ID.AM-03 states organizations must "maintain baselines of communication and data flows between the organization and third parties" and "maintain documentation of expected network ports, protocols, and services that are typically used among authorized systems."

NIST SP 800-53, Revision 5, Control CA-03 states organizations must "document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated …."

NIST SP 800-53, Revision 5, Control CA-09 states organizations must "document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated …."

NIST SP 800-53, Revision 5, Control CM-08 states organizations must "develop and document an inventory of system components that: Accurately reflects the system …."

Failure to maintain an accurate inventory increases the risk that systems and assets may not be properly secured, monitored, patched, assessed, or included in incident response and contingency planning activities.

Recommendation 1

We recommend that OPM review and update the FISMA inventory in the agency's governance, risk, and compliance tool, Archer, to reconcile the conflicts with the interconnection and public-facing component fields.

OPM Response:

"Concur. OPM is taking steps to address this recommendation and will provide supporting artifacts to demonstrate these actions."

OIG Comment

As a part of the audit resolution process, please provide the OIG with evidence that OPM has fully implemented this recommendation. This statement also applies to the subsequent recommendations in this audit report that OPM agrees to implement.

Metric 8 – Hardware Inventory

FY 2026 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.

Additionally, OPM consistently reports at least 80% of its government-furnished equipment through DHS' Continuous Diagnostics and Mitigation program as required by OMB Memorandum M-23-03.

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 2026 Maturity Level: 2 – Defined. OPM has defined policies, procedures, and processes for developing and maintaining an up-to-date inventory of software assets and licenses connected to OPM's network. OPM's documentation requires detailed information necessary for tracking and reporting, as well as critical, cloud, and mobile software.

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

Metric 10 – Data Inventory

FY 2026 Maturity Level: 2 – Defined. OPM has developed policies and procedures for maintaining a comprehensive and accurate inventory of data and corresponding metadata. This includes data obtained from third parties.

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

Metric 11 – Risk Policy and Strategy

FY 2026 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 and the Cybersecurity Risk Management Strategy. Within the Implementation Procedures and Guidelines: Risk Management Framework, 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 Cyber Resiliency Assessment and its plan of action and milestones. OPM also employs a cybersecurity risk register to manage risks and is consistently capturing and sharing lessons learned on the effectiveness of its cybersecurity risk program.

Furthermore, OPM uses tools to consistently monitor the effectiveness of risk responses to ensure that risk tolerances are maintained at an appropriate level. Through the use 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 2026 Maturity Level: 4 – Managed and Measurable. Through the Plan of Action & Milestones (POA&M) guide and Information Security Continuous Monitoring (ISCM) Plan, OPM has identified and defined the requirements for an automated solution that 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, 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 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.

OPM's overall maturity level for the Configuration Management domain is "2 – *Defined*."

The sections below detail the results for each individual metric in this domain.

Metric 14 – Security Configuration Settings

OPM has not documented, reviewed, and approved deviations from the baseline configurations.

FY 2026 Maturity Level: 2 – Defined. OPM has documented and maintains security configuration baselines for all operating platforms. OPM asserts that exceptions or deviations from the baseline configurations are managed through its risk management and system authorization process. OPM's Implementation Procedures and Guidelines: Risk Management Framework states that any operational obstacles, such as deviations, can be identified during the control implementation step. However, Security Content Automation Protocol–based compliance scans of Windows Server hosts revealed multiple compliance check failures against the applicable baseline. The organization could not demonstrate that these specific failed settings were documented, reviewed, and approved as exceptions within the authorization process.

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

The NIST SP 800-53, Revision 5, control CM-6 states that the organization must "identify, document, and approve any deviations …." Unapproved deviations from the secure baseline increase the system's attack surface and the likelihood of exploitable misconfigurations. Considering the failures are not tied to documented risk acceptances, OPM cannot demonstrate that residual risk was evaluated and formally accepted by the authorizing official, undermining the reliability of the authorization process and potentially the system's authorization status. This weakens overall configuration management assurance and the regulatory/compliance posture.

Recommendation 2

We recommend that OPM reconcile Security Content Automation Protocol scan failures and formally document any legitimate deviations.

OPM Response

"Concur. OPM is taking steps to address this recommendation and will provide supporting artifacts to demonstrate these actions."

Metric 15 – Flaw Remediation

FY 2026 Maturity Level: 2 – Defined. The OCIO has defined its implementation procedures and guidelines for system and information integrity that describe its flaw remediation parameters.

OPM has not consistently identified, prioritized, tested, and installed patches in a timely manner.

OPM also has a Cybersecurity and Privacy Policy that states that critical and high-severity vulnerabilities are to be patched within 30 days of discovery, consistent with its assertion of operation at the *Consistently Implemented* maturity level for flaw remediation. However, our review of vulnerability scan reports identified that high and critical vulnerabilities were not remediated within established timeframes. Specifically, 268 vulnerabilities were more than 60 days old, 40 high/critical vulnerabilities remained unpatched for more than 90 days, and 242 high/critical vulnerabilities were more than 120 days old after detection. These conditions indicate that patches, hotfixes, and updates were not consistently identified, prioritized, tested, and installed in a timely manner as required by the organization's 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 following recommendation is to assist OPM with attaining the *Consistently Implemented* maturity level.

The NIST SP 800-53, Revision 5, control SI-2 states the organization must identify, report, and correct system flaws; … test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; … [and] install security-relevant updates within [the organization-defined time period] of release …. The presence of unremedied high and critical vulnerabilities well beyond the organization's 30-day patching requirement significantly increases the risk that threat actors could exploit known vulnerabilities for which patches are publicly available.

Recommendation 3

We recommend that OPM implement a remediation approach such as a plan of action and milestones or a formal risk-based acceptance decision for any vulnerabilities that cannot be patched within the required timeframe.

OPM Response

"Concur. Although this is a long-term effort, OPM is taking steps to address this recommendation and will provide supporting artifacts to demonstrate these actions."

Metric 16 – Configuration Management Other Information

We have no additional comments regarding the Configuration Management program.

F. IDENTITY AND ACCESS MANAGEMENT

The Federal Identity and Access Management program is a governmentwide effort to help federal agencies provision access to systems and facilities to the right person, at the right time, for the right reason.

OPM's overall maturity level for the Identity and Access Management domain is "3 – *Consistently Implemented*."

The sections below detail the results for each individual metric in this domain.

Metric 17 – Multi-Factor Authentication

FY 2026 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented strong multifactor authentication (MFA) mechanisms for non-privileged users of the organization's physical and logical assets, including remote access to networks. Additionally, public-facing systems consistently use phishing-resistant MFA. While OPM's process for conducting digital identity risk assessments relies on a withdrawn NIST publication, OPM is within the timeframe defined by OMB Circular A-130 to update the process.

Non-privileged users are required to authenticate using strong MFA.

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 2026 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented strong MFA mechanisms for privileged users of the organization's physical and logical assets and networks. This includes remote access to networks. While the process for conducting the digital identity risk assessments relies on a withdrawn NIST publication, OPM is within the timeframe defined by OMB Circular A-130 to update the process.

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 2026 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented its policies for provisioning, managing, and reviewing privileged accounts. These processes cover approval and tracking, inventorying and validating, and logging and reviewing privileged users' accounts. OPM also limits the functions that can be performed when using privileged accounts and limits the duration that privileged accounts can remain logged in.

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 sensitive agency data.

OPM's overall maturity level for the Data Protection and Privacy domain is "3 – *Consistently Implemented*."

The sections below detail the results for each individual metric in this domain.

Metric 21 – Data Protection and Privacy Policies and Procedures

FY 2026 Maturity Level: 3 – Consistently Implemented. OPM has defined and communicated policies and procedures for encryption of data at rest, encryption of data in transit, removable 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.

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 22 – Data Exfiltration Prevention

FY 2026 Maturity Level: 3 – Consistently Implemented. OPM monitors the performance of its data exfiltration prevention and network defense controls through tool dashboards that capture both qualitative and quantitative measures. OPM also participates in Cybersecurity and Infrastructure Security Agency's (CISA) Continuous Diagnostics and Mitigation Program to strengthen its cybersecurity posture, and it uses CISA's Protective Domain Name System (DNS) for all external DNS queries. OPM asserted that its risk management framework procedures require applicable systems and services to undergo penetration tests. However, OPM submitted only a data loss prevention test dated 2023. Despite our request for more recent results, as of the date of this report OPM had not provided clarification, updated test results within the scope of this audit, or penetration test results demonstrating that it conducts routine exfiltration exercises.

OPM has not conducted routine exfiltration exercises.

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

NIST SP 800-53, Revision 5, Control SC-7(10), Boundary Protection | Prevent Exfiltration, requires the organization to: "(a) prevent the exfiltration of information; and (b) conduct exfiltration tests [at an organization-defined frequency]." Without current penetration testing and/or routine exfiltration exercises, OPM cannot demonstrate that its data loss prevention and boundary protection controls operate effectively against evolving threats. Undetected control weaknesses increase the risk that sensitive information could be exfiltrated from OPM's network without timely detection or prevention.

Recommendation 4

We recommend that OPM conduct penetration tests and data exfiltration exercises to demonstrate that its boundary protection and data loss prevention controls are operating effectively.

OPM Response

"Non-Concur. OPM is currently conducting penetration tests and data exfiltration exercises, as appropriate, and will provide supporting artifacts to more adequately demonstrate this."

OIG Comment

Once OPM provides supporting artifacts that the agency conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses, OPM OIG will be able to close this recommendation.

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. In addition, employees with IT security responsibilities are required to take specialized training specific to their job function.

OPM's overall maturity level for the Security Training domain is "3 – *Consistently Implemented*."

This section details the results for the metric in this domain.

Metric 24 – Security Training

FY 2026 Maturity Level: 3 – Consistently Implemented. OPM has defined its process for assessing the knowledge, skills, and abilities of its workforce to determine its specialized training needs and periodically updates its assessment to account for a changing risk environment.

OPM has conducted a Skills Gap Analysis to assess and identify gaps in the knowledge of its workforce.

Further, OPM has conducted a skills gap analysis to assess and identify gaps in the knowledge, skills, and abilities of its workforce related to 92 competencies. OPM identified critical competency gaps that should be prioritized and developed action plans to address the gaps. OPM then used the results of this as key input in its Cybersecurity Awareness and Training Strategy Fiscal Years 2026–2027.

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 25 – Security Training Other Information

We have no additional comments regarding the Security Training program.

I. INFORMATION SECURITY CONTINUOUS MONITORING

ISCM metrics address the controls related to performing ongoing information system assessments.

OPM's overall maturity level for the Information Security Continuous Monitoring domain (Detect) is "2 – *Defined*."

The sections below detail the results for each individual metric in this domain.

Metric 26 – ISCM Strategies and Policies

FY 2026 Maturity Level: 2 – Defined. During the third quarter of FY 2026, OPM developed and communicated a new Information System Continuous Monitoring Implementation Plan. The plan establishes monitoring requirements at each organizational tier, defines minimum monitoring frequencies, and describes an approach for ongoing control assessments. Under this approach, OPM is to annually select a subset of controls from the applicable NIST SP 800-53B baseline and document the controls in an Annual Assessment Plan. OPM subsequently provided an Annual Assessment Plan covering its FISMA

OPM has not conducted the assessments identified in the *Annual Assessment Plan*.

systems. However, OPM did not provide evidence that it conducted the assessments identified in the plan.

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

NIST SP 800-53, Revision 5, control CA-2 requires organizations to "assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements …." The OCIO Implementation Plan: Information System Continuous Monitoring requires OPM to annually select and evaluate a subset of controls from the applicable NIST SP 800-53B baseline and to document them in an annual assessment plan for each FISMA system.

Although OPM has developed an annual assessment plan, it has not conducted the assessments identified in the plan. Until it does, ongoing control assessments may be inconsistent, incomplete, or misaligned with the organization's actual risk environment. As a result, the organization may not assess the required controls on the schedule established by its ISCM plan, may not accurately determine whether security controls are operating as intended, may overlook deficiencies relevant to its specific risk posture, and may make risk-based decisions on incomplete or unreliable assessment information.

Recommendation 5

We recommend that OPM conduct assessments of the controls identified in its Annual Assessment Plan for each FISMA system in accordance with its policy and procedures.

OPM Response

"Non-Concur. OPM is currently conducting controls assessments according to its annual assessment plan and will provide supporting artifacts to more adequately demonstrate this."

OIG Comment

During audit fieldwork, OPM provided evidence of an annual assessment plan and stated that it was executed. However, no evidence was received that demonstrated the plan had been executed for any FISMA system. We continue to recommend that OPM provides the OIG with evidence of its implementation.

Metric 27 – ISCM Measuring Integrity and Security Posture

FY 2026 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 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 2026 Maturity Level: 2 – Defined. OPM has established system-level continuous monitoring strategies and supporting policies that govern how the agency conducts ongoing security control assessments, authorizes its systems to operate, maintains current system security plans, and monitors the security controls implemented for each individual system. These system-level strategies and policies also extend monitoring to security controls that fall outside the scope of OPM's organization-level ISCM strategy.

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

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.

OPM's overall maturity level for the Incident Response domain is "3 – *Consistently Implemented*."

The sections below detail the results for each individual metric in this domain.

Metric 30 – Incident Detection and Analysis

FY 2026 Maturity Level: 3 – Consistently Implemented. 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.

Additionally, OPM consistently captures and shares lessons learned on the effectiveness of its incident detection policies and procedures and makes updates as necessary. In the FY 2026 FISMA Metrics, OPM was required to achieve Event Logging Tier EL1 (basic) in accordance with OMB Memorandum M-21-31. However, in May of 2026, M-21-31 was rescinded by OMB Memorandum M-26-14, with M-26-14 serving as the new criteria for FISMA.

While OPM has achieved a minimum of Initial (Level 1) across all elements of the maturity model, the new M-26-14 standards require OPM to achieve Advanced (Level 3). However, according to M-26-14 and CIGIE Guidance, OPM is not required to complete and begin implementing these requirements until FY 2027. We will determine if OPM is in compliance with the new requirements during the FY 2027 FISMA audit.

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 31 – Incident Handling

FY 2026 Maturity Level: 2 – Defined. 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 implemented these playbooks when responding to incidents.

OPM is not capturing and protecting all incident data and metadata.

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 performance measures is obtained accurately, consistently, and in a reproducible format.

However, OPM conducted a Logging Gap Assessment to determine its Continuous Event Monitoring and Threat Hunting, Investigation, Response, and Forensics capabilities. This assessment indicated that eight systems are still being onboarded, and four High Value Assets still have coverage gaps. Additionally, all 51 systems still need a system-level assessment to verify their onboarding status. These gaps demonstrate OPM is not capturing and protecting all incident data and metadata at an enterprise-wide level.

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

NIST CSF RS.AN-07 states organizations must ensure, "Incident data and metadata are collected, and their integrity and provenance are preserved[.]" Failure to properly capture and

protect all incident data and metadata increases the duration of an incident and decreases the effectiveness of the responder's actions.

Recommendation 6

We recommend that OPM complete the onboarding and intake of all applicable systems and ensure that all incident data and metadata are captured at an enterprise-wide level.

OPM Response

"Non-concur. OPM believes that Agency Logging Plan (ALP) aligns with M-26-14 and the finalized Logging Reference Architecture (LRA), and will provide artifacts to more clearly demonstrate this."

OIG Comment

OPM's documentation demonstrated that the Logging Analysis, Visibility, and Automation Tracker did not reflect OPM's current state and that a new logging initiative is being implemented based on M-26-14. However, eight systems are still being properly onboarded (seven in progress and one in remediation), some of the onboarded systems have coverage gaps, and the onboarding state is pending per-system assessment, so systems may not be properly onboarded. We continue to recommend that OPM provides the OIG with evidence of implementation.

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.

OPM's overall maturity level for the Contingency Planning domain is "3 – *Consistently Implemented*."

The sections below detail the results for each individual metric in this domain.

Metric 33 – Business Impact Analysis

FY 2026 Maturity Level: 2 – Defined. OPM has defined its policies, procedures, and processes for conducting organizational and system-level business impact analyses (BIAs) and for incorporating the results into strategy and plan development efforts, such as information system contingency plans (ISCPs).

Fifteen system-level BIAs have not been incorporated into the ISCPs.

However, our testing found that OPM did not incorporate the recovery metrics from 15 system-level BIAs into the ISCPs.

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-2 states that the organization must "develop a contingency plan for the system that … identifies essential mission and business functions and associated contingency requirements; [and] provides recovery objectives, restoration priorities, and metrics." Failure to consistently implement the results of BIAs into system-level ISCPs could lead to increased downtime and poor decision-making during unexpected system and/or enterprise-wide disruptions.

Recommendation 7

We recommend that OPM incorporate the recovery metrics from 15 system-level BIAs into the ISCPs.

OPM Response

"Non-concur. OPM believes that required recovery objectives are incorporated into its BIAs and ISCPs and will provide supporting artifacts to more adequately demonstrate this."

OIG Comment

Based on our testing, we found that OPM did not incorporate the recovery metrics from 15 system-level BIAs into the ISCPs. In two instances, no BIA and/or ISCP were found. OPM OIG will review any supporting artifacts OPM provides to demonstrate it incorporated the BIAs.

Metric 34 – Contingency Plan Testing

FY 2026 Maturity Level: 3 – Consistently Implemented. OPM has defined its policies, procedures, and processes for 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.

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 35 – ISCP 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**

Metric Name	Self-Assessment FY 2026	Goal FY 2027	OIG Assessment FY 2025	OIG Assessment FY 2026	Function Score	Recommendation	Rolled Forward	New
Cybersecurity Governance	**3**	**3**	**2**	**3**				
Cybersecurity Profiles	3	3	1	3		No	N/A	N/A
Cybersecurity Risk Management	3	3	2	3		No	N/A	N/A
Cybersecurity Roles	3	3	3	3		No	N/A	N/A
Cybersecurity Governance Additional Information	N/A	N/A	N/A	N/A	**3**	No	N/A	N/A
Cybersecurity Supply Chain Risk Management (C-SCRM)	**3**	**3**	**3**	**3**				
Adherence to Cybersecurity and Supply Chain Requirements	3	3	3	3		No	N/A	N/A
C-SCRM Additional Information	N/A	N/A	N/A	N/A		No	N/A	N/A
Risk and Asset Management (RAM)	**3.17**	**3.17**	**2.83**	**2.83**				
Inventory of Major Systems and System Interconnections	4	4	4	2		Yes	N/A	1
Hardware Inventory	3	3	3	3		No	N/A	N/A
Software Inventory	2	2	1	2	**2.5**	No	N/A	N/A
Data Inventory	2	2	1	2		No	N/A	N/A
Risk Policy and Strategy	4	4	4	4		No	N/A	N/A
Centralized Enterprise-wide Risk Tool	4	4	4	4		No	N/A	N/A
Risk and Asset Management Other Information	N/A	N/A	N/A	N/A		No	N/A	N/A
Configuration Management	**3**	**3**	**1.5**	**2**				
Security Configuration Settings	3	3	1	2		Yes	N/A	1
Flaw Remediation	3	3	2	2		Yes	N/A	1
Configuration Management Other Information	N/A	N/A	N/A	N/A	**2.75**	No	N/A	N/A
Identity and Access Management (IDAM)	**3**	**3**	**3**	**3**				
Multi-Factor Authentication	3	3	3	3		No	N/A	N/A
Strong Authentication Mechanisms for Privileged Users	3	3	3	3		No	N/A	N/A
Management of Privileged User Accounts	3	3	3	3		No	N/A	N/A

Identity and Access Management Other Information	N/A	N/A	N/A	N/A		No	N/A	N/A
Data Protection and Privacy	**3.5**	**3.5**	**2**	**3**				
Data Protection and Privacy Policies and Procedures	3	3	2	3		No	N/A	N/A
Data Exfiltration Prevention	4	4	2	3		Yes	N/A	1
Data Protection and Privacy Other Information	N/A	N/A	N/A	N/A		No	N/A	N/A
Security Training	**3**	**3**	**2**	**3**				
Security Training	3	3	2	3		No	N/A	N/A
Security Training Other Information	N/A	N/A	N/A	N/A		No	N/A	N/A
Information Security Continuous Monitoring (ISCM)	**2.33**	**2.33**	**2**	**2**				
ISCM Strategies and Policies	3	3	2	2		Yes	N/A	1
ISCM Measuring Integrity and Security Posture	2	2	2	2	**2**	No	N/A	N/A
ISCM Ongoing Security Assessments	2	2	2	2		No	N/A	N/A
ISCM Other Information	N/A	N/A	N/A	N/A		No	N/A	N/A
Incident Response (IR)	**3.5**	**3.5**	**3**	**2.5**				
Incident Detection and Analysis	3	3	2	3	**2.5**	No	N/A	N/A
Incident Handling	4	4	4	2		Yes	N/A	1
Incident Response Other Information	N/A	N/A	N/A	N/A		No	N/A	N/A
Contingency Planning (CP)	**3**	**3**	**2.5**	**2.5**				
Business Impact Analysis	3	3	3	2	**2.5**	Yes	N/A	1
Contingency Plan Testing	3	3	2	3		No	N/A	N/A
ISCP Other Information	N/A	N/A	N/A	N/A		No	N/A	N/A
				Total Recommendations:			**0**	**7**

APPENDIX II – Status of Prior OIG Audit Recommendations

The table below outlines the status of recommendations issued in the FY 2025 FISMA audit (Report No. 2025-ISAG-008).			
Rec #	**Recommendation**	**Recommendation History**	**Current Status**
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.	New in 2025	CLOSED 5/1/26
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.	New in 2025	CLOSED 8/12/26
3	We recommend that OPM develop policies and procedures for developing and maintaining software inventory.	New in 2025	CLOSED 5/5/26
4	We recommend that OPM develop policies and procedures for developing and maintaining a data inventory.	New in 2025	CLOSED 10/13/26
5	We recommend that OPM document the settings/common secure configurations for all operating systems implemented within its environment.	New in 2025	CLOSED 5/18/26
6	We recommend that OPM remediate all data in transit vulnerabilities that the agency is currently tracking with plan of action and milestones.	New in 2025	CLOSED 4/2/26
7	We recommend that OPM ingest security logs from its FISMA systems and analyze events and anomalies.	New in 2025	CLOSED 10/13/26
8	We recommend that OPM update its literacy, awareness, and role-based training content using the results from workforce assessments and skills gap analyses.	New in 2025	CLOSED 4/30/26
9	We recommend that OPM document POA&Ms for all ISCM risks.	New in 2025	CLOSED 6/18/26
10	We recommend that OPM document lessons learned to improve its ISCM policies and strategy.	New in 2025	CLOSED 8/12/26
11	We recommend that OPM update its ISCM strategies to include policies and procedures to monitor its cloud service providers' security posture.	New in 2025	CLOSED 10/13/26
12	We recommend that OPM configure the agency logs/logging tools to meet the EL1 (basic) logging requirements outlined in M-21-31.	New in 2025	CLOSED 6/5/26
13	We recommend that OPM test all ISCPs annually as required by OPM policy.	New in 2025	CLOSED 10/13/26

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Chief Information
Officer

October 2, 2026

MEMORANDUM FOR: Eric Keehan
Office of the Inspector General

FROM: Adam Starr
Chief Information Officer

SUBJECT: Management's Response to the Audit Report of the Federal Information Security Modernization Act – FY 2026

The Office of the Chief Information Officer (CIO) appreciates the opportunity to review and provide a response to the audit report of the Federal Information Security Modernization Act (FISMA) Fiscal Year (FY) 2026, Report No. 2026-ISAG-003. The Office of the CIO values not only the open dialogue and partnership with the Office of the Inspector General (OIG), but also the forward thinking and diagnostic approach to this audit effort as a whole. Our responses to the recommendations are below.

Recommendation 1: We recommend OPM review and update the FISMA inventory in Archer to reconcile the conflicts with the Interconnection and Public Facing component fields.

Management's Response: Concur. OPM is taking steps to address this recommendation and will provide supporting artifacts to demonstrate these actions.

Recommendation 2: We recommend that OCIO reconcile security content automation protocol scan failures and formally document any legitimate deviations.

Management's Response: Concur. OPM is taking steps to address this recommendation and will provide supporting artifacts to demonstrate these actions.

Recommendation 3: We recommend that OCIO implement a remediation approach such as a plan of action and milestones or a formal risk-based acceptance decision for any vulnerabilities that cannot be patched within the required timeframe.

Management's Response: Concur. Although this is a long-term effort, OPM is taking steps to address this recommendation and will provide supporting artifacts to demonstrate these actions.

Recommendation 4: We recommend that OPM conduct penetration tests and data exfiltration exercises to demonstrate that its boundary protection and data loss prevention controls are operating effectively.

Management's Response: Non-Concur. OPM is currently conducting penetration tests and data exfiltration exercises, as appropriate, and will provide supporting artifacts to more adequately demonstrate this.

Recommendation 5: We recommend that OCIO conduct assessments of the controls identified in its Annual Assessment Plan for each FISMA system in accordance with its policy and procedures.

Management's Response: Non-Concur. OPM is currently conducting controls assessments according to its annual assessment plan and will provide supporting artifacts to more adequately demonstrate this.

Recommendation 6: We recommend that OPM complete the onboarding and intake of all applicable systems and ensure that all incident data and metadata are captured at an enterprise-wide level.

Management's Response: Non-concur. OPM believes that Agency Logging Plan (ALP) aligns with M-26-14 and the finalized Logging Reference Architecture (LRA), and will provide artifacts to more clearly demonstrate this.

Recommendation 7: We recommend that OPM incorporate the recovery metrics from 15 system level BIAs into the ISCPs.

Management's Response: Non-concur. OPM believes that required recovery objectives are incorporated into its BIAs and ISCPs and will provide supporting artifacts to more adequately demonstrate this.
cc:

Doug McKain
Acting 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/contact/hotline

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. 2026-ISAG-003