



**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 2023**

**Report Number 2023-ISAG-006
November 22, 2023**

EXECUTIVE SUMMARY

Federal Information Security Modernization Act Audit - Fiscal Year 2023

Report No. 2023-ISAG-006

November 22, 2023

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 remotely from December 2022 through August 2023 in Washington, D.C.



Michael R. Esser
*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 Cybersecurity Framework. The Cybersecurity Framework is comprised of nine "domain" areas and the weighted averages of the domain scores are used to derive the agency's overall cybersecurity score. In fiscal year 2023, 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 nine domains from the five cybersecurity framework functional areas:

Risk Management – OPM has defined an enterprise-wide risk management strategy through its risk management council. OPM has developed and implemented policies, procedures, and processes to maintain up-to-date inventory of its hardware and software.

Supply Chain Risk Management – OPM has defined and communicated an organization-wide Supply Chain Risk Management (SCRM) strategy that addresses risk appetite and tolerance, strategies and controls, processes for consistently evaluating and monitoring supply chain risk, and approaches for implementing and communicating the SCRM strategy.

Configuration Management – OPM has developed, documented, and disseminated baseline configurations and standard configuration settings for its information systems. The agency has an established configuration change control process.

Identity, Credential, and Access Management (ICAM) – OPM provided a comprehensive ICAM strategy and Charter detailing its goals and objectives. OPM has enforced multi-factor authentication with Personal Identity Verification cards.

Data Protection and Privacy – OPM has established the Office of Privacy and Information Management, which has defined and communicated OPM’s privacy program plan and related policies and procedures. However, OPM has not consistently dedicated appropriate resources to the program or ensured that individuals are consistently performing the privacy roles and responsibilities that have been defined across OPM.

Security Training – OPM has implemented a security training strategy and program. OPM stated that there were no new resource gaps within their workforce; however, a current gap analysis needs to be provided to demonstrate any weaknesses in specialized training.

Information Security Continuous Monitoring (ISCM) – OPM has established ISCM policies for its environment. OPM’s continuous monitoring strategies address security control monitoring at the organization, business unit, and individual information system levels. However, OPM does not consistently document lessons learned to make improvements to the ISCM policies and strategy.

Incident Response – OPM has implemented many of the required controls for incident response. Based upon our audit work, OPM has successfully implemented all the FISMA metrics at the level of *Managed and Measurable*.

Contingency Planning – OPM has implemented several of the FISMA requirements related to contingency planning and continues to improve upon maintaining its contingency plans as well as conducting contingency plan tests on a routine basis.

ABBREVIATIONS

Authorization	Security Assessment and Authorization
BIA	Business Impact Analysis
CDM	Continuous Diagnostics and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISO	The Chief Information Security Officer
CITAR	Capital Investments and IT Acquisition Review
CM	Configuration Management
CRMS	Cybersecurity Risk Management Strategy
DHS	U.S. Department of Homeland Security
FICAM	Federal Identity, Credential, and Access Management
FIPS	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
GRC	Governance, Risk, and Compliance
ICAM	Identity, Credential, and Access Management
IG	Inspector General
ISCM	Information Security Continuous Monitoring
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	U.S. Office of Management and Budget
OPIM	Office of Privacy and Information Management
OPM	U.S. Office of Personnel Management
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
SCRM	Supply Chain Risk Management
SP	Special Publication
TIC	Trusted Internet Connection
VDP	Vulnerability Disclosure Policy

TABLE OF CONTENTS

EXECUTIVE SUMMARY	i
ABBREVIATIONS	iii
I. BACKGROUND	1
II. OBJECTIVE, SCOPE, AND METHODOLOGY	2
III. AUDIT FINDINGS AND RECOMMENDATIONS	6
A. Introduction and Overall Assessment	6
B. Risk Management	8
C. Supply Chain Risk Management	12
D. Configuration Management	14
E. Identity, Credential, and Access Management	18
F. Data Protection and Privacy.....	22
G. Security Training	24
H. Information Security Continuous Monitoring	27
I. Incident Response	29
J. Contingency Planning	32
APPENDIX I: Detailed FISMA Results by Metric	
APPENDIX II: Status of Prior OIG Audit Recommendations	
APPENDIX III: The Office of Personnel Management’s October 13, 2023, response to the draft audit report, issued September 29, 2023.	
REPORT FRAUD, WASTE, AND MISMANAGEMENT	

I. BACKGROUND

The 2002 Federal Information Security Management Act required (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 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 IGs in fulfilling their FISMA evaluation and reporting responsibilities, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in coordination with OMB, issued the Inspector General Reporting Metrics. This document provides a methodology and format for agencies to report FISMA audit results to the U.S. Department of Homeland Security (DHS). It identifies a series of reporting topics that relate to specific agency responsibilities outlined in FISMA.

The FISMA IG Reporting Metrics utilize 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.

We would also like to highlight the fact that of the 29 recommendations in last year's FISMA audit report, the OCIO staff were able to close all but 2 by the end of this year's audit. This is an exceptional achievement that we greatly appreciate.

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:

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

We also performed audits focused on two of OPM's major information systems – the Benefits Plus and Enterprise Mainframe systems.

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) 2023.

Like the prior two 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 FY 2024. 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 future maturity level it intends to achieve by the end of FY 2024 if it was higher than the current 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 to varying degrees on 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:

- OPM Information Technology Security FISMA Procedures;
- OPM Security Assessment and Authorization (Authorization) Guide;
- OPM Plan of Action and Milestones Guide;
- OMB Circular A-130, Managing Information as a Strategic Resource;
- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive 12;

- P.L. 107-347, Title III, Federal Information Security Management Act of 2002;
- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- NIST Special Publication (SP) 800-12, Revision 1, An Introduction to Computer Security: The NIST Handbook;
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-37, Revision 2, Guide for Applying the Risk Management Framework to Federal Information Systems;
- NIST SP 800-39, Managing Information Security Risk – Organization, Mission, and Information System View;
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems;
- NIST SP 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60, Volume 2, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories;
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information;
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems;
- Federal Information Processing Standards Publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;
- Federal Information System Controls Audit Manual; and

- FIPS 140-2, Security Requirements for Cryptographic Modules.

The OPM Office of the Inspector General, established by the Inspector General Act of 1978, as amended, performed the audit from December 2022 through August 2023 in OPM's Washington, D.C. office.

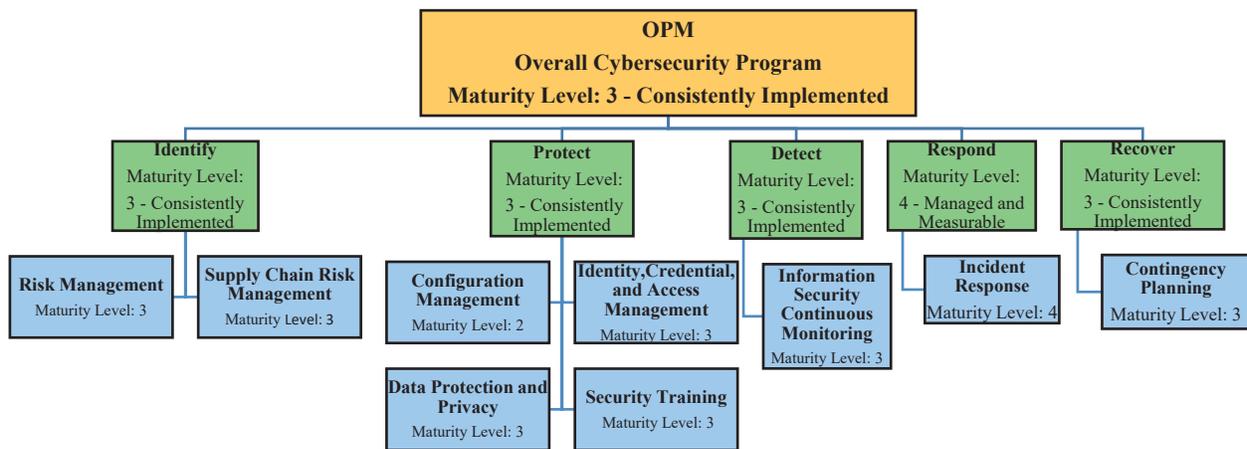
COMPLIANCE WITH LAWS AND REGULATIONS

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 IG Reporting Metrics use a maturity model evaluation system derived from the NIST Cybersecurity Framework. The Cybersecurity Framework is comprised of five “function” areas that map to the nine “domains” under the function areas. These nine 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 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 IG FISMA Reporting Metrics:

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

Level 4: <i>Managed and Measurable</i>	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: <i>Optimized</i>	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.

In previous years, Inspector Generals (IGs) 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 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 analyses of the data obtained through this pilot and the FY2020 – FY2022 governmentwide IG 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, the ratings below were from FY 2023 and were based on a calculated average approach, wherein the average of the metrics in a particular domain was used to determine the effectiveness of individual function areas (*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.

Function	Core	FY23 Supplemental	FY24 Supplemental	FY23 Assessed Maturity
Identify	2.83	3.20	2.67	Consistently Implemented (Level 3)
Protect	2.63	2.60	2.88	Consistently Implemented (Level 3)
Detect	2.50	3.00	3.00	Consistently Implemented (Level 3)
Respond	4.00	4.00	4.00	Managed and Measurable (Level 4)
Recover	2.50	3.00	2.00	Consistently Implemented (Level 3)
Overall Maturity	2.89	3.16	2.91	Consistently Implemented (Level 3)

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

B. RISK MANAGEMENT

Risk management controls are the tools, policies, and procedures that enable an organization to understand and control risks associated with its IT infrastructure and services. These controls should be implemented throughout the agency and used to support making risk-based decisions with limited resources. The sections below detail the results for each individual metric in this domain. **OPM’s overall maturity level for the Risk Management domain is “3 – Consistently Implemented.”**

Metric 1 – Inventory of Major Systems and System Interconnections

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM has policies and procedures for developing an inventory of information systems. OPM policy states that Information System Security Officers (ISSO) are responsible for generating system registration forms. The registration forms are used to inventory internal and external information systems. Public-facing websites, cloud systems, and interconnections are inventoried as a part of the authorization process. Interconnections are inventoried as a part of OPM’s Information Security Continuous Monitoring (ISCM) strategy. OPM monitors and maintains the inventories and interconnection records in its Governance, Risk, and Compliance (GRC) tool, Archer. The Chief Information Security Officer (CISO) and ISSOs are responsible for ensuring that inventory monitoring processes follow OPM’s ISCM strategy. The CISO is tasked with establishing and overseeing monitoring procedures and inventory. The ISSO is responsible for carrying out the procedures and updating the inventory.

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

Metric 2 – Hardware Inventory

FY 2023 Maturity Level: 2 – Defined. OPM’s Secure Asset Management Policy requires that infrastructure managers develop and document an inventory of information system components. The policy includes specific data elements/taxonomy information such as manufacturer, type, model, serial number, and physical location. OPM also uses multiple tools to manually capture standard data elements following defined and documented procedures and processes.

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

Metric 3 – Software Inventory

FY 2023 Maturity Level: 2 – Defined. OPM has developed and implemented policies, procedures, and processes to maintain an up-to-date software inventory. Currently, OPM leverages its Business Case Exception and Application Whitelist processes to develop and maintain its software inventory. However, OPM recognizes that its current process could be improved and has drafted a plan to establish a more authoritative software inventory solution. OPM performs quarterly reviews of its software inventory in accordance with its processes and procedures documented in the CIO FISMA Metrics Standard Operating Procedures.

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

Metric 4 – System Security Categorization

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM has policies and procedures in place to categorize its systems. ISSOs document the security categorization of their systems based on FIPS 199, NIST SP 800-60, and OPM guidance. The OPM Security Authorization Guide requires that system owners, authorizing officials and the Chief Information Security Officer are involved with approving the security categorization of systems. OPM utilizes its Enterprise Business Impact Analysis to prioritize the recovery of systems, along with the identification and prioritization of high value assets and activities. Systems that are categorized as high risk or high value assets are allocated more ISSOs. Through this action OPM has demonstrated that they are allocating resources through a data-driven prioritization and system categorization.

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

Metric 5 – Risk Policy and Strategy

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has defined its policies, procedures, and processes to manage cybersecurity risks through its Risk Management Policy and Cybersecurity Risk Management Strategy (CRMS). Through the issuance of the CRMS and development of other resources, OPM has defined policies, procedures, and processes for risk framing, risk assessment, risk response, and risk monitoring. OPM consistently meets the threshold for completing risk assessments within the organizationally defined time frame.

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

Metric 6 – Information Security Architecture

FY 2023 Maturity Level: 2 – Defined. OPM has defined its information security architecture by establishing a three-tiered approach which is comprised of information security architecture at the Agency tier, the Program tier, and the System tier. OPM’s Enterprise Architecture document and Security Reference Model define this information security architecture. OPM has also developed a System and Service Acquisition Policy and FISMA Procedures that define system security engineering principles and software assurance processes for mobile applications. Additionally, the System and Service Acquisition Policy and FISMA Procedures define and document the roles, responsibilities, and security controls that ensure appropriate security principles are included in OPM’s systems development life cycle process. Adherence to security engineering principles is accomplished through the completion of OPM’s Security Impact Analysis and Security Assessment processes.

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

Metric 7 – Risk Management Roles, Responsibilities, and Resources

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM has defined and communicated the roles and responsibilities of stakeholders involved in the cybersecurity risk management process through risk management policies, the CRMS, and the Risk Management Council (RMC) Charter. The CRMS was developed in accordance with the Enterprise Risk Management Strategy to ensure risk management roles are in alignment between the two strategies. OPM ensures communication of roles and responsibilities related to cybersecurity risk management through its SharePoint site, which stores all documents (e.g., policies, templates, processes, procedure guides) related to risk management. The RMC meets routinely and provides input on the cybersecurity risk register. OPM performance standards ensure accountability of cybersecurity personnel and program managers with risk management responsibilities such as allocating resources and implementing risk management processes.

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

Metric 8 – Plan of Action and Milestones

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has implemented and communicated policies and procedures for the effective use of Plan of Action and Milestones (POA&M). The policies and procedures address the centralized tracking of security weaknesses, prioritization of remediation efforts, maintenance, and independent validation of POA&M activities. OPM has a consistent approach to POA&Ms using risk assessments, security categorizations, control deficiencies, and risk ratings. Using Archer as a risk repository, OPM utilizes POA&Ms to effectively track and mitigate security weaknesses. Dashboards in Archer allow OPM to see the number of POA&Ms in various stages such as initial, draft, and open.

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

Metric 9 – Risk Communication

FY 2023 Maturity Level: 3 – Consistently implemented. OPM defines how cybersecurity risks are communicated in a timely manner to all necessary internal and external stakeholders, through a multitude of cybersecurity risk management policies, procedures, and strategies. OPM documents its cybersecurity risks as POA&Ms captured in its GRC tool, Archer. POA&Ms are documented with required criteria, as defined by the OPM POA&M Guide, as a part of the tool. ISSOs are responsible for supporting System Owners and Business Program Managers with regards to the management and communication of the POA&Ms. OPM also created enterprise continuous monitoring metrics around POA&Ms to support timely communication and management of cybersecurity risks. An Archer dashboard collects real-time data from the system and is reviewed on a weekly basis.

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

Metric 10 – Centralized Enterprise-wide Risk Tool

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM has implemented a GRC tool to provide a centralized enterprise-wide view of risks across OPM. This would include risk control, remediation activities, dependencies, risk levels, and management dashboards. Through the POA&M guide and ISCM strategy, OPM has defined the requirements for an automated solution which provides a centralized enterprise-wide view of cybersecurity risks. The POA&M guide provides OPM with a standardized process to identify, document, manage, and remediate

risk/weakness within OPM. The guide specifically details the process a risk goes through in Archer, and all the various stages needed to be completed before a risk can be resolved. OPM's ISCM strategy defines the extent to which POA&Ms are to be used in Archer, and how Archer will be used for FISMA system inventory and security control assessments. Archer is currently live and serving as an automated solution across the agency. It also serves as a repository that stores information regarding FISMA System Inventory, along with all risk controls and remediation activities associated with a system. Furthermore, in Archer, risk scores and levels are identified for systems, along with having a management dashboard.

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

Metric 11 – Risk Management Other Information

We have no additional comments regarding risk management.

C. SUPPLY CHAIN RISK MANAGEMENT

The Supply Chain Risk Management (SCRM) metrics deal with SCRM strategy throughout the organization. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the SCRM domain is "3 – Consistently Implemented."**

Metric 12 – SCRM Strategy

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has defined and communicated an organization wide SCRM strategy by publishing SCRM Implementation Procedures and Guidelines. The document identifies OPM's SCRM strategy that addresses risk appetite and tolerance, strategies and controls, processes for consistently evaluating and monitoring supply chain risk, and approaches for implementing and communicating the SCRM strategy. This document is stored on OPM's SharePoint site allowing for communication of the SCRM strategy to reach stakeholders.

The RMC is used by OPM to consistently implement the SCRM strategy. The RMC conducts discussions that address the limitations, challenges, and effective management of supply chain risk. OPM also utilizes lessons learned to identify potential improvements to OPM's SCRM strategy.

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

Metric 13 – SCRM Policies and Procedures

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has consistently implemented the agency’s SCRM strategy and System Acquisition Policy that includes procedures, scope, roles and responsibilities, and baseline supply chain related controls. The SCRM Implementation Procedures and Guidelines document security policies, baseline configurations, IT acquisition guidance, and implementation instructions for agency-wide use. Lessons learned by the RMC are documented to support the efforts by OPM to review and update its SCRM policies, procedures, and processes.

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

Metric 14 – Adherence to Cybersecurity and Supply Chain Requirements

FY 2023 Maturity Level: 2 – Defined. OPM has defined and communicated policies and procedures to ensure products, system components, systems, and services adhere to its cybersecurity SCRM requirements. OPM’s documented SCRM Implementation Procedures and Guidelines define the risk mitigation strategies for the acquisition process of hardware, commercial off-the-shelf software, custom software supported by contract, open-source software, and services. To confirm contractors are meeting their contractual SCRM obligations, OPM Contracting Officers review contractors past performance.

OPM’s SCRM Implementation Procedures and Guidelines: System and Service Acquisition defines the acquisition process and mandates the usage of the Capital Investments and IT Acquisition Review (CITAR) application. All IT-related acquisitions are required to enter and progress through the CITAR review and approval process. OPM's Implementation Procedures and Guidelines require system owners to ensure contracts require vendors to design new systems using cybersecurity and privacy principles (e.g., least privilege, layered protection, boundary protection, etc.). Standardized language is provided by the OCIO that can be incorporated into agency contracts, which can define and document government oversight through monthly, quarterly, annual, and ad hoc deliverables (e.g., monthly reports that confirm contractors are complying with SCRM obligations).

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

Metric 15 – Component Authenticity

FY 2023 Maturity Level: 2 – Defined. OPM’s SCRM Implementation Procedures and Guidelines define and communicate its component authenticity policy and procedures. Our review of this document determined that OPM has addressed procedures (e.g., out-of-band hashes, encryption, digital signature, transmission security) to detect and prevent counterfeit

components from entering the system. Additionally, OPM’s SCRM Implementation Procedures and Guidelines defines procedures to maintain configuration control over organizationally defined components awaiting repair or service and requirements and procedures for reporting counterfeit system components.

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

Metric 16 – SCRM Additional Information

We have no additional comments regarding SCRM.

D. 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.”**

Metric 17 – Configuration Management Roles, Responsibilities, and Resources

FY 2023 Maturity Level: 2 – Defined. OPM demonstrated that individual roles and responsibilities for configuration management were defined through OPM policies and procedures and communicated across the agency.

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

Metric 18 – Configuration Management Plan

FY 2023 Maturity Level: 2 – Defined. OPM has defined and documented enterprise level configuration management policies and procedures that outline roles and responsibilities, institute a change control board, and define processes for implementing configuration changes. However, the agency has not integrated its overall configuration management plan into its continuous monitoring and risk management programs. OPM has also not established a process to document lessons learned from the implementation of its configuration management activities to make improvements to the plan.

OPM does not integrate its overall configuration management plan into its continuous monitoring and risk management programs.

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

this metric as *Defined*. The recommendation below is to assist OPM with attaining the *Consistently Implemented* maturity level.

NIST SP 800-128 states that “An information system is composed of many components How these system components are networked, configured, and managed is critical in providing adequate information security and supporting an organization’s risk management process.”

Without an integrated enterprise configuration management plan and documented lessons learned, there is an increased risk that the configuration management process will not effectively manage the system security settings that protect OPM’s environment.

Recommendation 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.

OPM’s Response:

“Concur. OPM will continually mature our configuration management through further integration with OPM’s Enterprise Risk Management (ERM) program. We will also evaluate our IT control continuous monitoring program to ensure we achieve the maturity level goal of 3 - Consistently Implemented.”

OIG Comment:

As part of the audit resolution process, we recommend that OPM provide OPM’s 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 19 – Baseline Configurations

FY 2023 Maturity Level: 2 – Defined. OPM has begun implementing a process to migrate information systems to a cloud environment. OPM has developed, documented, and disseminated its baseline configuration and component inventory policies and procedures for all information systems in use by OPM. The baseline configuration documents are approved for distribution and contain the scope, document renewal and review timeline, applicable regulations, and minimum configuration settings for each information system. These baseline configurations are published on the OCIO-Cyber SharePoint site for all designated personnel to access.

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

Metric 20 – Security Configuration Settings

FY 2023 Maturity Level: 2 – Defined. OPM has developed, documented, and disseminated its policies and procedures in the form of hardening guides that define configuration settings and common secure configurations tailored specifically to OPM’s environment. Additionally, OPM has established a process to document and track deviations from the hardening guides.

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

Metric 21 – Flaw Remediation and Patch Management

FY 2023 Maturity Level: 2 – Defined. OPM has defined and documented a Patch Management Policy and configuration management policies and procedures. However, during testing, we identified vulnerabilities for the mainframe that were not remediated within 30 days, as required by the Patch Management Policy.

OPM does not ensure security patches are implemented within 30 days per its Patch Management Policy.

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

OPM’s Patch and Vulnerability Management Policy states that security-relevant software and firmware updates need to be installed not to exceed 30 days after the release of the updates.

NIST SP 800-53, Revision 5, states that an organization should “Identify, report, and correct system flaws ...” and “Install security-relevant software and firmware updates within [organization-defined time period] after the release of the updates.”

Without a formal process to scan and track the remediation of known vulnerabilities, there is a significantly increased risk that systems will indefinitely remain susceptible to attack.

Recommendation 2 (Rolled forward from 2021)

We recommend that the OCIO implement a process to apply critical operating system and third-party vendor patches in a 30-day window according to OPM policy.

OPM’s Response:

“Concur. OPM is updating IT security policies and procedures to meet National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5. OPM will also further centralize the patching processes and review and update the patching procedures as

necessary. Once final and after several months of successful implementation, we will provide the updated documentation to OIG.”

Metric 22 – Trusted Internet Connection Program

FY 2023 Maturity Level: 1 – Ad Hoc. OPM provided a Trusted Internet Connection (TIC) Implementation Plan, as well as documentation to support its initial development of use cases for a TIC. However, OPM did not provide an accurate inventory of its network connections and TIC use case documentation that outlined which alternative security controls, such as endpoint and user-based protections, must be in place for specific scenarios in which traffic may not be required to flow through a physical TIC access point for all information systems.

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

OMB Memorandum M-19-26 states that agency “Chief Information Officers shall maintain an accurate inventory of agency network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, and topological data for each connection in the event OMB, DHS, or others request this information to assist with governmentwide cybersecurity incident response or other cybersecurity matters.”

OMB Memorandum M-19-26 also states that “TIC Use Case documentation will outline which alternative security controls, such as endpoint and user-based protections, must be in place for specific scenarios in which traffic may not be required to flow through a physical TIC access point.”

Failure to document an accurate inventory and TIC use cases for all information systems increases the risk that OPM cannot maintain the high level of security needed to protect networks from malicious actors.

Recommendation 3

We recommend that OPM maintain an accurate inventory of its network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, use cases, and topological data for the agency’s TIC process.

OPM’s Response:

“Concur. We will update the current TIC implementation plan and inventory of external connections. We will also address the details outlined in the recommendation. We will provide the updated documentation to OIG once it is available.”

Metric 23 – Configuration Change Control Management

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has developed and documented policies and procedures for controlling configuration changes. The policies address the necessary change control steps and documentation required to approve information system changes. Our test work indicated that OPM has updated its configuration change control process to include project plans and additional reviews and approvals and is consistently adhering to its change control procedures.

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

Metric 24 - Vulnerability Disclosure Policy

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has a Vulnerability Disclosure Policy (VPD) as part of its vulnerability management program for internet-accessible Federal systems. The policy addresses the scope, types of testing allowed, reporting mechanisms, timely feedback, and remediation efforts of the agency’s vulnerability research programs. OPM has also demonstrated that it consistently implements its VDP. In addition, OPM has updated the relevant fields at the .gov registrar to ensure appropriate reporting by the public, ensured that all internet-accessible systems are included in the scope of its VDP, and increased the scope of systems covered by its VDP, in accordance with DHS Binding Operational Directive 20-01.

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

Metric 25 – Configuration Management Other Information

We have no additional comments regarding configuration management.

E. IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

The Federal Identity, Credential, and Access Management program is a government-wide effort to help Federal agencies provision access to systems and facilities for 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, Credential, and Access Management domain is “3 – Consistently Implemented.”**

Metric 26 – ICAM Roles, Responsibilities, and Resources

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has individual policies and procedures that define roles and responsibilities for specific aspects of Identity, Credential, and

Access Management (ICAM). OPM has developed an ICAM strategy to align and consolidate the agency’s ICAM investments, monitor programs, and ensure awareness and understanding. Roles and responsibilities for all users are incorporated in a comprehensive ICAM strategy.

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

Metric 27 – ICAM Strategy

FY 2023 Maturity Level: 2 – Defined. OPM has defined and documented a comprehensive ICAM Strategy and Charter detailing its goals/milestones and objectives. However, OPM has not demonstrated progress toward meeting its milestones and has not submitted lessons learned that are incorporated into its ICAM Policy.

OPM does not have documented lessons learned that are incorporated into its ICAM Policy.

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

OMB Memorandum M-19-17 states that “Each agency shall define and maintain a single comprehensive ICAM policy, process, and technology solution roadmap, consistent with agency authorities and operational mission needs. These items should encompass the agency's entire enterprise, align with the Government-wide Federal Identity, Credential, and Access Management (FICAM) Architecture and CDM requirements, incorporate applicable Federal policies, standards, playbooks, and guidelines”

The absence of documentation that demonstrates ICAM progress increases the risk that OPM will not successfully meet major milestones and achieve the Federal ICAM initiatives.

Recommendation 4

We recommend that OPM develop and implement a roadmap or other documentation that contains progress in meeting milestones.

OPM’s Response:

“Concur. The OPM Zero Trust Strategy 2.0 contains a roadmap and was provided to the OIG during audit fieldwork. OPM will link the ICAM strategy and milestones to the roadmap. We will provide the revised documentation after several months.”

Recommendation 5

We recommend OPM document lessons learned that are incorporated into its ICAM Policy.

OPM's Response:

“Concur. OPM began documenting lessons learned for the ICAM strategy in the later part of FY23 with the intent of potential incorporation into the ICAM policy or strategy. We have provided the lessons learned documentation to OIG under separate cover.”

Metric 28 – Personnel Risk

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented processes for assigning personnel risk designations and performing appropriate screenings prior to granting access to its systems. Additionally, OPM re-screens individuals when they change positions, or the risk designation of their current position is changed.

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

Metric 29 – Access Agreements

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented centralized processes for developing, documenting, and maintaining access agreements for all users of the network. All personnel are required to review and acknowledge access agreements prior to being granted initial access to systems and on an annual basis thereafter, as a part of IT Security and Privacy Awareness training.

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

Metric 30 – Multi-factor Authentication with PIV

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM enforces multi-factor authentication for non-privileged users of its facilities, systems, and networks using Personal Identity Verification (PIV) cards. This includes remote access to networks. Digital identity risk assessments are performed for each system to ensure that authentication processes provide the appropriate level of assurance.

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

Metric 31 – Strong Authentication Mechanisms for Privileged Users

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM enforces multi-factor authentication for privileged users of its facilities, systems, and networks using PIV cards. OPM utilizes tools including an enterprise password vault to manage privileged user access to the OPM network and its back-end servers. Digital identity risk assessments are performed for each system to ensure that authentication processes provide the appropriate level of assurance.

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

Metric 32 – Management of Privileged User Accounts

FY 2023 Maturity Level: 1 – Ad Hoc. OPM has not defined its process for provisioning, managing, and reviewing privileged user accounts. OPM has developed a server operation procedure template and privileged account request forms. However, a defined process should include approval, tracking, inventorying, validating, logging, and reviewing privileged users' accounts.

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

NIST SP 800-53, Revision 5, states that the organization “Develop, document and disseminate ... Procedures to facilitate the implementation of the access control policy and associated access controls”

Failure to develop privileged access procedures increases the risk that implementation of the access control policy and associated access controls will not be effective.

Recommendation 6 (Rolled Forward from FY 2021)

We recommend that OPM define its process for provisioning, managing, and reviewing privileged accounts.

OPM's Response:

“Concur. OPM reviewed and updated our existing procedures and documentation related to provisioning, managing, and reviewing privileged accounts. We will provide the documents to OIG once the documents are final.”

Metric 33 – Remote Access Connections

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has implemented a variety of controls for remote access connections such as the use of approved cryptographic modules, system time outs, and event logging. OPM ensures that FIPS 140-2 validated cryptographic modules are implemented for its remote access connection methods, remote access sessions time out after 30 minutes, and that remote users’ activities are logged and reviewed based on risk.

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

Metric 34 – ICAM Other Information

We had no additional information about OPM's ICAM program.

F. DATA PROTECTION AND PRIVACY

The Data Protection and Privacy metrics deal with the controls over the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems. 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 “3 – Consistently Implemented.”**

Metric 35 – Data Protection and Privacy Policies and Procedures

FY 2023 Maturity Level: 2 – Defined. OPM has established the Office of Privacy and Information Management (OPIM). OPIM has defined and communicated its privacy program plan and related policies and procedures for the protection of PII that is collected, used, maintained, shared, and/or disposed of by OPM’s information systems. In addition, roles and responsibilities for the effective implementation of the organization’s privacy program have been defined and the organization has determined the resources and optimal governance structure needed to effectively implement its privacy program.

OPM does not have appropriate resources for its privacy program.

However, although OPM has added two Presidential Management Fellows to the privacy team in FY 2023, OPM has not consistently dedicated appropriate resources to the program and ensured that individuals are consistently performing the privacy roles and responsibilities that have been defined across OPM.

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

this metric as *Defined*. The recommendation below is to assist OPM with attaining the *Consistently Implemented* maturity level.

OMB Circular A-130 states, “Implement policies and procedures to ensure that all personnel are held accountable for complying with agency-wide information security and privacy requirements and policies” OMB A-130 also states, “Identify and plan for the resources needed to implement information security and privacy programs”

Failure to consistently implement a privacy program increases the agency’s risk for data loss and mishandling of sensitive information.

Recommendation 7

We recommend that OPM consistently utilize resources that perform the privacy roles and responsibilities that have been defined across OPM.

OPM’s Response:

“Concur. The Office of the Executive Secretariat and Privacy and Information Management (OESPIM) agrees that additional resources are needed for the Privacy program at OPM. The demand for privacy reviews and compliance on new projects and pilots has increased with new technological strides, increased data capabilities, and the expansion of our data-sharing outreach. We had intended to add two Presidential Management Fellows (PMF) to OESPIM during FY23, but the start date for the first PMF was deferred to late October of FY24. We now plan to employ a Direct Hire instead of a second PMF later in FY24. We also seek additional hires to meet the growing demand for Privacy reviews of deliverables.

While we have established a framework that provides for the exercise of the privacy roles and responsibilities across OPM, we plan to take additional steps to continually increase consistency, taking into account competing priorities and resource constraints.”

Metric 36 – Data Protection and Privacy Controls

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM’s policies and procedures have been consistently implemented for the specified areas, including (i) use of FIPS-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit, (ii) prevention and detection of untrusted removable media, and (iii) destruction or reuse of media containing PII or other sensitive agency data.

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

Metric 37 – Data Exfiltration Prevention

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM has defined policies to prevent data exfiltration from its IT environment and to implement enhanced network defenses. OPM has implemented controls to monitor inbound and outbound network traffic, as well as ensure that all traffic passes through a web content filter. In addition, OPM has implemented a process to measure the effectiveness of the controls on an ongoing basis.

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

Metric 38 – Data Breach Response Plan

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has consistently implemented its Data Breach Response Plan and has participated in table-top exercises. OPM has also documented lessons learned within an Incident Report Form. Additionally, OPM has utilized a Breach Response Team that can identify specific individuals affected by a breach, send notice to the affected individuals, and provide those individuals with credit monitoring and repair services, as necessary.

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

Metric 39 – Privacy Awareness Training

FY 2023 Maturity Level: 2 – Defined. OPM has defined and communicated its Privacy Awareness Training Program Policy and is consistent with NIST criteria. This policy describes role-based privacy training distributed on an annual basis. OPM has tailored annual privacy training which is distributed to the OPM workforce.

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

Metric 40 – Data Protection and Privacy Other Information

We had no additional information about OPM's data protection controls or privacy program.

G. SECURITY TRAINING

FISMA requires that all Government employees and contractors take annual IT security awareness training. In addition, employees with IT security responsibility are required to take specialized training specific to their job function. OPM has a strong history of providing its

employees with IT security awareness training for the ever-changing risk environment and has made progress in providing tailored training to those with significant security responsibilities. The sections below detail the results for each individual metric in this domain. **OPM’s overall maturity level for the Security Training domain is “3 – Consistently Implemented.”**

Metric 41 – Security Training Policies and Procedures

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has established an agency-wide IT security awareness training program. Roles and responsibilities for stakeholders are defined and communicated across the agency. OPM continues to mature its security training program by consistently collecting and analyzing performance measures of the training activities.

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

Metric 42 – Assessment of Workforce

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM stated that there were no new resource gaps within their workforce. However, a current gap analysis to identify any weaknesses in specialized training has not been conducted. The analysis should define work roles and document gaps between the optimal proficiency level and current proficiency level.

OPM needs to conduct a current gap analysis to identify any weaknesses in specialized training.

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

The Federal Cybersecurity Workforce Assessment Act of 2015 requires agencies to implement “a strategy for mitigating any gaps identified ... with the appropriate training and certification for existing personnel.” The Cybersecurity Workforce Assessment Act of 2015 also states that “annually thereafter through 2022, the head of each Federal agency ... shall ... identify information technology, cybersecurity, or other cyber-related work roles of critical need in the agency’s workforce; and ... submit a report to the Director that ... describes the information technology, cybersecurity, or other cyber-related roles,” as well as “substantiates the critical need designations.”

Failure to identify gaps within an IT security training program increases the risk that OPM staff are not fully prepared to address the security threats facing the agency.

Recommendation 8

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.

OPM's Response:

“Concur. OPM will continue to conduct and update the workforce assessment in FY24. To meet our goal of the managed and measurable maturity level, we will build on our existing procedures by ensuring that targeted training and talent acquisition are incorporated and executed. As this is demonstrated and documented, OPM will provide evidence to OIG.”

Metric 43 – Security Awareness Strategy

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has developed a security awareness and training strategy that is consistently implemented to maintain a security awareness program tailored to the mission and risk environment. OPM also continues to conduct a gap analysis and periodic reassessment of organizational skills related to security awareness and training.

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

Metric 44 – Tracking IT Security Training

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM has defined and tailored its security awareness policies, procedures, and related material and delivery methods based on FISMA requirements and the types of information systems that its users have access to. In addition, the organization has defined its processes for ensuring that all information system users, including contractors, are provided security awareness training within organizationally defined timeframes, and periodically thereafter. Furthermore, the organization has:

- Defined its processes for evaluating and obtaining feedback on its security awareness and training program and using that information to make continuous improvements;
- Ensured that its security awareness policies and procedures are consistently implemented. OPM ensures that all appropriate users complete the organization's security awareness training (or a comparable awareness training for contractors) [within organizationally defined timeframes] and periodically thereafter, and maintains completion records;
- Obtained feedback on its security awareness and training program and uses that information to make improvements;
- Measured the effectiveness of its awareness program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate;

- Monitored and analyzed qualitative and quantitative performance measures on the effectiveness of its security awareness policies, procedures, and practices; and
- Ensured that data supporting metrics are obtained accurately, consistently, and in a reproducible format.

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

Metric 45 – Tracking Specialized IT Security Training

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM employees with significant information security responsibilities are required to take specialized security training in addition to the annual awareness training. The OCIO uses a database to track the security training taken by employees identified as having security responsibility. One example of the specialized training program involves the OCIO conducting targeted phishing exercises/emails for individuals with security responsibilities, tracking the exercise results, and following up as needed.

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

Metric 46 – Security Training Other Information

We have no additional comments regarding the security training program.

H. INFORMATION SECURITY CONTINUOUS MONITORING

ISCM controls involve the ongoing assessment of control effectiveness in support of the agency’s efforts to manage information security vulnerabilities and threats. The sections below detail the results for each individual metric in this domain. **OPM’s overall maturity level for the Information Security Continuous Monitoring domain is “3 – Consistently Implemented.”**

Metric 47 – ISCM Policies Strategy

FY 2023 Maturity Level: 2 – Defined. OPM has established ISCM policies for its environment. OPM’s continuous monitoring strategies address security control monitoring at the organization, business unit, and individual information system levels. At the organization and business unit levels, the ISCM strategies define how the agency’s activities support risk management in accordance with organizational risk tolerance. At

OPM does not document lessons learned to make improvements to its ISCM policies and strategy.

the information system level, the ISCM program has established processes for monitoring security controls for effectiveness and reporting any findings. However, OPM does not consistently document lessons learned to make improvements to the ISCM policies and strategy.

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

NIST SP 800-137, states that an organization’s continuous monitoring program will “evolve with lessons learned and with increased insight into organizational security status and risk tolerance.”

Failure to document ISCM progress increases the risk that OPM will not successfully meet major milestones and achieve the Federal ISCM initiatives.

Recommendation 9

We recommend that OPM document lessons learned that are incorporated into its ISCM policies and strategy.

OPM’s Response:

“Concur. As OPM works to mature to a ‘Consistently Implemented’ level across several metrics and domains, lessons learned is an important component of maturation. We will incorporate the current lessons learned template and actions in the ISCM policies and strategy.”

Metric 48 – ISCM Roles, Responsibilities, and Resources

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has established policies and procedures to describe its ISCM configuration, roles, and duties for its ISCM team. OPM has ensured that its workforce is performing ISCM responsibilities with its utilization of ISCM reports and dashboards.

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

Metric 49 – Ongoing Security Assessments

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has consistently implemented its processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls for individual systems.

1) Controls Testing

We found that all systems are following the security control-testing schedule that the OCIO has mandated. OPM is reporting the security status of information systems to the CIO and Authorizing Official for the systems at least quarterly.

2) System Authorizations

We reviewed 51 system authorizations that contained Ongoing Security Authorization schedules, POA&Ms, System Security Plans, Security Assessment Reports, and Authority to Operate letters, and have concluded OPM has established its processes for performing system authorizations.

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

Metric 50 – Measuring ISCM Program Effectiveness

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. In addition, OPM has defined the format of reports, frequency of reports, and the tools used to provide information to individuals with significant security responsibilities. The ISCM program includes POA&Ms, Authorizations, and ongoing security controls assessments. OPM has demonstrated that it is capturing the qualitative and quantitative performance measures for POA&Ms and Authorizations. We also observed qualitative and quantitative performance measures captured for the systems that completed the ongoing security controls assessments.

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

Metric 51 – ISCM Other Information

We have no additional comments regarding OPM’s ISCM program.

I. INCIDENT RESPONSE

Incident response is an organized approach for responding to cyber-attacks in an effective manner and limiting the damage, repair costs, and down time of critical information systems. OPM has an effective incident response program. The sections below detail the results for each individual metric in this domain. **OPM’s overall maturity level for the Incident Response domain is “4 – Managed and Measurable.”**

Metric 52 – Incident Response Policies, Procedures, Plans, Strategies

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM’s incident response policies, procedures, plans, and strategies have been defined, communicated, and consistently implemented. OPM monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response program and is consistently capturing and sharing lessons learned to implement updates to the program as appropriate.

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

Metric 53 – Incident Roles and Responsibilities

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM has defined roles and responsibilities related to incident response, and its incident response teams have adequate resources (people, processes, and technology) to manage and measure the effectiveness of incident response activities.

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

Metric 54 – Incident Detection and Analysis

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM employs a classification system for its incident response program to efficiently analyze and prioritize any reportable or detectable incidents. It has implemented security tools with the ability to analyze activity patterns to identify precursors and indicators of threats, which detect and prevent intrusions. OPM has developed profiling techniques on its networks and systems to detect security incidents more effectively. OPM also monitors and analyzes the qualitative and quantitative performance measures on the effectiveness of its incident detection and analysis policies and procedures.

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

Metric 55 – Incident Handling

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM has defined its processes for incident handling in an Incident Response Manual. The processes include containment strategies for various types of major incidents, eradication activities to eliminate components of an incident and mitigation techniques for exploited vulnerabilities. OPM uses metrics to measure the impact

of successful incidents and is quickly able to mitigate related vulnerabilities on other systems so that they are not subject to the same exploitation.

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

Metric 56 – Sharing Incident Response Information

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM has a documented policy that defines how incident response information will be shared with individuals that have significant security responsibility. Controls are in place to ensure that security incidents are reported to DHS, law enforcement, the Office of the Inspector General, and Congress in a timely manner. OPM has developed and implemented incident response metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.

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

Metric 57 – Contractual Relationships in Support of Incident Response

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM collaborates with DHS and other parties, when needed, for technical assistance, surge resources, and any special requirements for quickly responding to incidents. OPM uses third party contractors, when needed, to support incident response processes. OPM also utilizes software tools provided by DHS for intrusion detection and prevention capabilities.

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

Metric 58 – Technology to Support Incident Response

FY 2023 Maturity Level: 4 – Managed and Measurable. OPM identified and fully defined its requirements for incident response technologies. OPM has implemented incident response tools to collect and retain data consistent with the agency's incident response policy, plans, and procedures. OPM utilizes the incident response tools to monitor and analyze qualitative and quantitative incident response performance measures across the agency. OPM uses the data collected from these tools to generate monthly reports for stakeholders on the effectiveness of its incident response program.

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

Metric 59 – Incident Response Other Information

We have no additional comments regarding OPM’s incident response capability.

J. 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 60 – Contingency Planning Roles and Responsibilities

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has a policy describing the agency’s contingency planning program roles and responsibilities as well as system-level contingency planning documents that assign individuals to specific recovery activities. To address gaps related to contingency planning activities, the role of system owners has been reevaluated and responsibilities will be communicated in a future Investment Review Board meeting.

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

Metric 61 – Business Impact Analysis

FY 2023 Maturity Level: 3 – Consistently Implemented. Identifying an organization’s essential mission and the risks facing its business functions are critical elements in developing contingency plans. OPM has defined its policies and procedures for conducting Business Impact Analyses (BIAs) and has performed an enterprise-level BIA and system-level BIAs for all its major systems. OPM uses a template to create all system-level BIAs.

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

Metric 62 – Contingency Plan Maintenance

FY 2023 Maturity Level: 2 – Defined. OPM has developed policies and procedures which define contingency plan development, maintenance, and integration with other continuity areas.

The process for developing information system contingency plans covers all relevant phases including activation, notification, recovery, and reconstitution. However, OPM does not have an information system contingency plan in place for 12 out of 51 of its systems. Additionally, existing information system contingency plans have not been reviewed and updated within the last year for 15 out of 51 systems.

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

NIST SP 800-34, Revision 1, states that “it is essential that the [information system contingency plan] be reviewed and updated regularly as part of the organization’s change management process to ensure that new information is documented, and contingency measures are revised if required.”

According to OPM’s Contingency Planning Policy, information system contingency plans must be updated annually.

Failure to maintain current and accurate contingency plans increases the risk that the agency will be unable to restore operations effectively and efficiently in the event of a service impacting incident.

Recommendation 10 (Rolled forward from 2014)

We recommend that the OCIO ensure that all of OPM’s major systems have contingency plans in place and that they are reviewed and updated annually.

OPM’s Response:

“Concur. Contingency plans are in place for IT systems. We have provided the remediation evidence to OIG.”

OIG Comment:

In response to the draft audit report, we received evidence that contingency plans for OPM’s major information systems were in place and reviewed/updated this fiscal year; no further action is required.

Metric 63 – Contingency Plan Testing

FY 2023 Maturity Level: 2 – Defined. Routine testing is a critical step in ensuring that contingency plans can be executed successfully in the event of a disaster. The ISCP Coordinator is responsible for developing the contingency plan test and overseeing the execution of that test.

As reported last year, OPM has not effectively performed annual contingency plan testing for all systems within its inventory since 2008. OPM has not tested the contingency plan for 17 out of its 51 information systems within the last year, in accordance with OPM policy. Out of the 17 contingency plans that were not tested within the last year, 5 had tests that were performed over one year ago, and 12 did not have a contingency plan test on record at all.

Additionally, during fieldwork we identified that OPM's contingency planning policies and procedures were missing required elements defined in NIST SP 800-34, Revision 1, and FISMA Reporting Metrics. These elements included notification procedures, internal and external connectivity, system performance using alternate equipment, or restoration of normal procedures. However, prior to the end of this audit, OPM has remediated this weakness by producing updated policies and procedures that include the necessary testing requirements. Therefore, we will not issue a recommendation for this policy and procedure finding.

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

NIST SP 800-53, Revision 5, states that the organization “Test the contingency plan for the system [at an organization defined frequency]”

OPM policy requires system owners to “Test the contingency plan for the information system [at least annually]” Failure to routinely perform sufficient contingency plan testing for every major information system increases the risk that the agency will be unable to restore operations effectively and efficiently in the event of a service-impacting incident.

Recommendation 11 (Rolled forward from 2008)

We recommend that OPM test the contingency plans for each system on an annual basis.

OPM’s Response:

“Concur. OPM has tested contingency plans for each system this fiscal year. We have provided evidence to OIG.”

OIG Comment:

In response to the draft audit report, we received evidence that contingency plans for OPM’s major information systems were tested this fiscal year; no further action is required.

Metric 64 – Information System Backup and Storage

FY 2023 Maturity Level: 2 – Defined. OPM has defined its policies, procedures, processes, strategies, and technologies for information system backup and storage, including the use of

alternate storage and processing sites and redundant array of inexpensive disks, as appropriate. The organization has considered alternative approaches when developing its backup and storage strategies, including cost, environment maximum downtimes, recovery priorities, and integration with other contingency plans.

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

Metric 65 – Communication of Recovery Activities

FY 2023 Maturity Level: 3 – Consistently Implemented. OPM has defined how the planning and performance of recovery activities are communicated to internal stakeholders and executive management teams. OPM has provided information on the planning and performance of recovery activities which are consistently communicated to relevant stakeholders and executive management teams, who utilize the information to make risk-based decisions.

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

Metric 66 – Contingency Planning Other Information

We have no additional comments regarding contingency planning.

APPENDIX I – Detailed FISMA Results by Metric

Metric Number and Description	Metric Maturity Level	Domain Maturity Level	Function Maturity Level	U.S. OPM Overall Maturity Level	
1 - Inventory of Major Systems and System Interconnections	4	Risk Management	Identify	Agency Overall	
2 - Hardware Inventory	2	Level 3: Consistently Implemented	Level 3: Consistently Implemented	Level 3: Consistently Implemented	
3 - Software Inventory	2				
4 - System Security Categorization	4				
5 - Risk Policy and Strategy	3				
6 - Information Security Architecture	2				
7 - Risk Management Roles, Responsibilities, and Resources	4				
8 - Plan of Action and Milestones	3				
9 - Risk Communication	3				
10 - Centralized Enterprise-wide Risk Tool	3				
11 - Risk Management Other Information -	n/a				
12 - SCRM Policies and Procedures	3				Supply Chain Risk Management
13 - Implementation of SCRM	3				
14 - Ensure 3rd parties follow SCRM Requirements	2	Level 3: Consistently Implemented			
15 - Maintaining and Monitoring SCRM	2				
16 - SCRM Other	n/a				
17 - Configuration Mgt. Roles, Responsibilities, and Resources	2	Configuration Management	Level 3: Consistently Implemented		
18 - Configuration Management Plan	2	Level 2: Defined			
19 - Baseline Configurations	2				
20 - Security Configuration Settings	2				
21 - Flaw Remediation and Patch Management	2				
22 - Trusted Internet Connection Program	1				
23 - Configuration Change Control Management	3				
24 - Vulnerability Disclosure Policy	3				
25 - Configuration Management Other Information	n/a				
26 - ICAM Roles, Responsibilities, and Resources	3	Identify and Access Management			Level 3: Consistently Implemented
27 - ICAM Strategy	2	Level 3: Consistently Implemented			
28 - Personnel Risk	3				
29 - Access Agreements	3				
30 - Multi-factor Authentication with PIV	3				
31 - Strong Authentication Mechanisms for Privileged Users	3				
32 - Management of Privileged User Accounts	1				
33 - Remote Access Connections	3				
34 - ICAM Other Information - Contractor Access Management	n/a				
35 - Data Protection and Privacy Policies and Procedures	2	Data Protection and Privacy	Level 3: Consistently Implemented		
36 - Data Protection and Privacy Controls	3				
37 - Data Exfiltration Protection	4				
38 - Data Breach Response Plan	3				
39 - Privacy Awareness Training	2				
40 - Other Information - Data Protection and Privacy	n/a				
41 - Security Training Policies and Procedures	3	Security Training	Level 3: Consistently Implemented		
42 - Assessment of Workforce	3				
43 - Security Awareness Strategy	3				
44 - Tracking IT Security Training	4				
45 - Tracking Specialized IT Security Training	4				
46 - Other Information - Security Training Program	n/a				
47 - ISCM Policies Strategy	2	Continuous Monitoring			Detect
48 - ISCM Roles, Responsibilities, and Resources	3	Level 3: Consistently Implemented			
49 - Ongoing Security Assessments	3				
50 - Measuring ISCM Program Effectiveness	3				
51 - ISCM Other Information	n/a				
52 - Incident Response Policies, Procedures, Plans, and Strategies	4	Incident Response	Respond	Level 4: Managed and Measurable	
53 - Incident Roles and Responsibilities	4	Level 4: Managed and Measurable			
54 - Incident Detection and Analysis	4				
55 - Incident Handling	4				
56 - Sharing Incident Response Information	4				
57 - Contractual Relationships in Support of Incident Response	4				
58 - Technology to Support Incident Response	4				
59 - Incident Response Other Information	n/a				
60 - Contingency Planning Policies and Procedures	3		Contingency Planning		Recover
61 - Business Impact Analysis	3		Level 3: Consistently Implemented		
62 - Contingency Plan Maintenance	2				
63 - Contingency Plan Testing	1				
64 - Information System Backup and Storage	2				
65 - Communication of Recovery Activities	3				
66 - Contingency Planning Other Information	n/a				

KEY

Red – Ad Hoc

Yellow – Defined

Green – Consistently Implemented or higher

APPENDIX II – Status of Prior OIG Audit Recommendations

The table below outlines the current status of recommendations issued in the FY 2022 FISMA audit (Report No. 2022-ISAG-0017, issued November 15, 2022).

Rec #	Original Recommendation	Recommendation History	Current Status
1	We recommend that OPM define the procedures for maintaining its hardware inventory.	Rolled forward from 2019	CLOSED 1/9/23
2	We recommend that OPM define policies and procedures for a centralized software inventory.	Rolled forward from FY 2018	CLOSED 10/18/23
3	We recommend that OPM complete risk assessments for each major information system that are compliant with NIST guidelines and OPM policy. The results of a complete and comprehensive test of security controls should be incorporated into each risk assessment.	Rolled forward from FY 2017	CLOSED 3/14/23
4	We recommend that OPM update its enterprise architecture, to include the information security architecture elements required by NIST and OMB guidance.	Rolled forward from FY 2017	CLOSED 4/12/23
5	We recommend that OPM improve its POA&M remediation process to ensure that at least 80% of open POA&Ms are closed within the risk-based remediation timeframes.	New recommendation in FY 2022	CLOSED 10/18/23
6	We recommend that OPM develop an action plan and outline its processes to address the supply chain risk management requirements of NIST SP 800-161	Rolled forward from FY 2019	CLOSED 8/10/23
7	We recommend that OPM perform a gap analysis to determine the configuration management resource requirements (people, processes, and technology) necessary to effectively implement the agency's CM program.	Rolled forward from FY 2017	CLOSED 11/17/22
8	We recommend that OPM document the lessons learned from its configuration management activities and update its configuration management plan as appropriate.	Rolled forward from FY 2017	CLOSED 10/18/23
9	We recommend that OPM develop and implement a baseline configuration for all information systems in use by OPM.	Rolled forward from FY 2017	CLOSED 4/17/23
10	We recommend that the OCIO develop and implement [standard security configuration settings] for all operating platforms in use by OPM.	Rolled forward from FY 2014	CLOSED 7/20/23

11	For OPM configuration standards that are based on a pre-existing generic standard, we recommend that OPM document all instances where the OPM-specific standard deviates from the recommended configuration setting.	Rolled forward from FY 2016	CLOSED 10/18/23
12	We recommend that the OCIO implement a process to apply critical operating system and third-party vendor patches in a 30-day window according to OPM policy.	Rolled forward from FY 2021	OPEN: ROLLED FORWARD AS REPORT 2023-ISAG-006 RECOMMENDATION 2
13	We recommend that the OCIO implement a process to ensure new server installations are included in the scan repository.	Rolled forward from FY 2018	CLOSED 6/6/23
14	We recommend that OPM establish an agency-wide TIC program to manage and maintain its external agency connections.	Rolled forward from FY 2021	CLOSED 7/20/23
15	We recommend that OPM create a charter to govern the roles and responsibilities of its ICAM office's governance body	Rolled forward from FY 2021	CLOSED 7/20/23
16	We recommend that OPM develop and implement an ICAM strategy that considers a review of current practices ("as-is" assessment) and the identification of gaps (from a desired or "to-be" state), and contains milestones for how the agency plans to align with Federal ICAM initiatives.	Rolled forward from FY 2017	CLOSED 7/20/23
17	We recommend that OPM define its process for provisioning, managing, and reviewing privileged accounts.	Rolled forward from FY 2021	OPEN: ROLLED FORWARD AS REPORT 2023-ISAG-006 RECOMMENDATION 6
18	We recommend that OPM establish and document configuration and connection requirements which must be met prior to authorizing remote access.	New recommendation in FY 2022	CLOSED 7/21/23
19	We recommend that OPM acquire the identified resources for the privacy program.	New recommendation in FY 2022	CLOSED 10/18/23
20	We recommend that OPM implement a process to ensure that individuals are consistently performing the privacy roles and responsibilities that have been defined across OPM.	Rolled forward from 2018	CLOSED 10/18/23
21	We recommend that OPM develop a process to routinely test the Data Breach Response Plan.	Rolled forward from FY 2018	CLOSED 10/18/23

22	We recommend that OPM identify individuals with heightened responsibility for PII and provide role-based training to these individuals at least annually.	Rolled forward from FY 2018	CLOSED 10/18/23
23	We recommend that OPM perform a gap-analysis to determine the contingency planning requirements (people, processes, and technology) necessary to effectively implement the agency's contingency planning policy.	Rolled forward from FY 2018	CLOSED 4/14/23
24	We recommend that OPM update the BIA Worksheet template to include all criteria outlined in NIST SP 800-34, Revision 1.	New recommendation in FY 2022	CLOSED 3/14/23
25	We recommend that the OCIO ensure that all of OPM's major systems have contingency plans in place and that they are reviewed and updated annually.	Rolled forward from FY 2014	CLOSED 10/18/23
26	We recommend that OPM update its policies and procedures for contingency plan testing to define requirements for all areas included in NIST SP 800-34, / Revision 1.	New recommendation in FY 2022	CLOSED 9/19/23
27	We recommend that OPM test the contingency plans for each system on an annual basis.	Rolled forward from FY 2008	CLOSED 10/18/23
28	We recommend that OPM perform and document an analysis of alternative backup and storage strategies including cost, maximum downtimes, security, recovery priorities, and integration with larger, organization-level contingency plans.	New recommendation in FY 2022	CLOSED 10/18/23
29	We recommend that OPM perform and document controls testing to ensure security safeguards for alternate processing and storage sites are equivalent to the primary sites.	Rolled forward from FY 2020	CLOSED 10/18/23

APPENDIX III



Office of the
Chief Information
Officer

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

October 13, 2023

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

FROM: Guy Cavallo
Chief Information Officer

Mark Flaster
Senior Agency Official for Privacy
Office of Privacy and Information Management

SUBJECT: Office of Personnel Management Response to the Office of
the Inspector General Federal Information Security
Modernization Act Audit – FY23
(Report No. 2022-ISAG-006)

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report, the Federal Information Security Modernization Act (FISMA) Fiscal Year 2023, Report No. 2022-ISAG-006. The OIG comments are valuable as they afford us the opportunity to independently assess our operations and help to inform our continuous efforts to enhance the privacy and security of the data that the Office of Personnel Management (OPM) receives and possesses.

We appreciate OIG's focus on continuous progress toward a fully matured cybersecurity and privacy posture as set forth by the FISMA maturity model and underlying metrics. The self-assessment is a useful tool to inform the actions required to improve our security and privacy posture. OPM will continue to work with OIG to achieve a mutual understanding of the use of the evolving FISMA maturity model and the underlying metrics that were introduced in Fiscal Year (FY) 2017.

This year, OPM concurs with 11 of the OIG's 11 recommendations.

Responses to your recommendations including planned corrective actions, as appropriate, are provided below.

Recommendation 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.

Management Response: Concur. OPM will continually mature our configuration management through further integration with OPM's Enterprise Risk Management (ERM) program. We will also evaluate our IT control continuous monitoring program to ensure we achieve the maturity level goal of 3 - Consistently Implemented.

Recommendation 2 (Rolled forward from 2021): We recommend that the OCIO implement a process to apply critical operating system and third-party vendor patches in a 30-day window according OPM policy.

Management Response: Concur. OPM is updating IT security policies and procedures to meet National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5. OPM will also further centralize the patching processes and review and update the patching procedures as necessary. Once final and after several months of successful implementation, we will provide the updated documentation to OIG.

Recommendation 3: We recommend that OPM maintain an accurate inventory of its network connections, including details on the service provider, cost, capacity, traffic volume, logical/physical configurations, use cases, and topological data for the agency's TIC process.

Management Response: Concur. We will update the current TIC implementation plan and inventory of external connections. We will also address the details outlined in the recommendation. We will provide the updated documentation to OIG once it is available.

Recommendation 4: We recommend that OPM develop and implement a roadmap or other documentation that contains progress in meeting milestones.

Management Response: Concur. The OPM Zero Trust Strategy 2.0 contains a roadmap and was provided to the OIG during audit fieldwork. OPM will link the ICAM strategy and milestones to the roadmap. We will provide the revised documentation after several months.

Recommendation 5: We recommend OPM document lessons learned that are incorporated into its ICAM Policy.

Management Response: Concur. OPM began documenting lessons learned for the ICAM strategy in the later part of FY23 with the intent of potential incorporation into the ICAM policy or strategy. We have provided the lessons learned documentation to OIG under separate cover.

Recommendation 6 (Rolled forward from 2021): We recommend that OPM define its process for provisioning, managing, and reviewing privileged accounts.

Management Response: Concur. OPM reviewed and updated our existing procedures and documentation related to provisioning, managing, and reviewing privileged accounts. We will provide the documents to OIG once the documents are final.

Recommendation 7: We recommend that OPM consistently utilize resources that perform the privacy roles and responsibilities that have been defined across OPM.

Management Response: Concur. The Office of the Executive Secretariat and Privacy and Information Management (OESPIM) agrees that additional resources are needed for the Privacy program at OPM. The demand for privacy reviews and compliance on new projects and pilots has increased with new technological strides, increased data capabilities, and the expansion of our data-sharing outreach. We had intended to add two Presidential Management Fellows (PMF) to OESPIM during FY23, but the start date for the first PMF was deferred to late October of FY24. We now plan to employ a Direct Hire instead of a second PMF later in FY24. We also seek additional hires to meet the growing demand for Privacy reviews of deliverables.

While we have established a framework that provides for the exercise of the privacy roles and responsibilities across OPM, we plan to take additional steps to continually increase consistency, taking into account competing priorities and resource constraints.

Recommendation 8: We recommend that OPM develop and conduct an updated assessment of its workforce's knowledge, skills, and abilities in order to identify any skill gaps and specialized training needs.

Management Response: Concur. OPM will continue to conduct and update the workforce assessment in FY24. To meet our goal of the managed and measurable maturity level, we will build on our existing procedures by ensuring that targeted training and talent acquisition are incorporated and executed. As this is demonstrated and documented, OPM will provide evidence to OIG.

Recommendation 9: We recommend OPM document lessons learned that are incorporated into its ISCM policies and strategy.

Management Response: Concur. As OPM works to mature to a "Consistently Implemented" level across several metrics and domains, lessons learned is an important

component of maturation. We will incorporate the current lessons learned template and actions in the ISCM policies and strategy.

Recommendation 10 (Rolled forward from 2014): We recommend that the OCIO ensure that all of OPM's major systems have contingency plans in place and that they are reviewed and updated annually.

Management Response: Concur. Contingency plans are in place for IT systems. We have provided the remediation evidence to OIG.

Recommendation 11 (Rolled forward from 2008): We recommend that OPM test the contingency plans for each system on an annual basis.

Management Response: Concur. OPM has tested contingency plans for each system this fiscal year. We have provided evidence to OIG.

We appreciate the opportunity to respond to the draft report and look forward to continuous collaboration to enhance data security and privacy. Please contact us if you have questions or need additional information.

cc:

Alethea Predeoux
Chief of Staff

Erica Roach
Chief Financial Officer, Acting

Mark Lambert
Associate Director, Merit System Accountability and Compliance
Director, Internal Oversight and Compliance

Melvin Brown
Deputy Chief Information Officer

Larry Allen
Associate Chief Information Officer, IT Strategy & Policy

James Saunders
Chief Information Security Officer

Webb Lyons
General Counsel



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: <http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse>

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