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 2022

Report Number 2022-ISAG-0017
November 15, 2022

Executive Summary

Federal Information Security Modernization Act Audit - Fiscal Year 2022

Report No. 2022-ISAG-0017 **October XX, 2021**

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 2021 through August 2022 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 FY 2022, 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 is working to implement a comprehensive inventory management process for its hardware and software inventories.

Supply Chain Risk Management – OPM's Supply Chain Risk Management program is *Ad-hoc* and needs to be developed.

Configuration Management – OPM continues to develop baseline configurations and approve standard configuration settings for its information systems. The agency has an established configuration change control process.

Identity, Credential, and Access Management (ICAM) – OPM is continuing to develop its agency ICAM strategy. OPM has enforced multi-factor authentication with Personal Identity Verification cards.

Data Protection and Privacy – OPM has defined controls related to data protection and privacy including data exfiltration prevention. However, the Data Breach Response Plan has not been updated or tested.

Security Training – OPM has implemented a security training strategy and program. OPM has performed a workforce assessment to identify the skill gaps for the agency's cybersecurity workforce.

Information Security Continuous Monitoring – OPM has established many of the policies and procedures surrounding continuous monitoring, but the agency has not consistently implemented all the Information Security Continuous Monitoring policies. OPM also needs to continue to improve its process for conducting security controls assessments on all its information systems.

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 not implemented several of the FISMA requirements related to contingency planning and needs 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**
CISO	**Chief Information Security Officer**
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**
IOC	**Internal Oversight and Compliance**
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**

Table of Contents

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

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

II. Objective, Scope, and Methodology

Objective

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

- 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 performed audits focused on one of OPM's major information systems – the Annuity Roll System.

Scope and Methodology

We conducted this performance audit in accordance with U.S. Government Accountability Office's Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit covered OPM's FISMA compliance efforts throughout FY 2022.

Like last year, we requested OPM to 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 hopes to achieve by the end of FY 2022. 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 2022 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 Guide;
- OPM Plan of Action and Milestones Standard Operating Procedures;
- OMB Circular A-130, Managing Information as a Strategic Resource;
- OMB Memorandum M-07-12, Preparing for and Responding to a Breach of Personally Identifiable Information;
- OMB Memorandum M-19-17: Enabling Mission Delivery through Improved Identity, Credential, and Access Management;
- OMB Memorandum M-19-26: Update to the Trusted Internet Connections (TIC) Initiative;
- P.L. 107-347, Title III, Federal Information Security Management Act of 2002;
- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- P.L. 115-390, SECURE Technology Act;

- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information 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;
- NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems; and
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance.

The OPM Office of the Inspector General, established by the Inspector General Act of 1978, as amended, performed the audit from December 2021 through August 2022 in OPM's Washington, D.C. office.

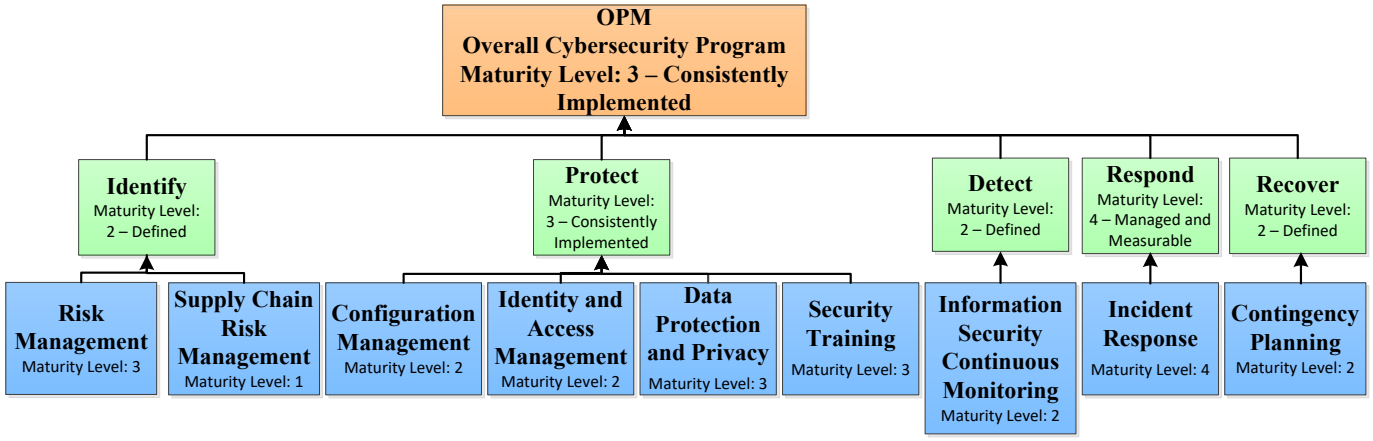
Compliance with Laws and Regulations

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 each function area. These nine domains are broad cyber security control areas used to assess the effectiveness of the information security policies, procedures, and practices of the agency. Each domain is comprised of a series of individual metrics, which are the specific controls that we evaluated and tested when assessing the agency's cybersecurity program. Each metric receives a maturity level rating of 1-5. The chart below outlines the overall maturity of OPM's cybersecurity program.



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

Maturity Level	Maturity Level Description
Level 1: *Ad Hoc*	Policies, procedures, and strategy are not formalized; activities are performed in an ad hoc, reactive manner.
Level 2: *Defined*	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: *Consistently Implemented*	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: *Managed and Measurable*	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.

Maturity Level	Maturity Level Description
Level 5: *Optimized*	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Last year, a new pilot concept of weighting certain metrics for scoring was introduced. This year we did not receive official guidance from DHS on the calculation method to determine the maturity levels of the domains, function areas and overall agency rating. In the absence of official guidance, we decided to continue using last year's method. These proposed priority metrics would be weighted twice as much in the maturity calculation and are listed below.

Metric	Description	Cybersecurity Function and Domain
5	Cybersecurity risk management and integration with enterprise risk management	Identify – Risk Management
10	Automated view of risk	Identify – Risk Management
31	Strong authentication measures – privileged users	Protect – Identity and Access Management
32	Least privilege and separation of duties	Protect – Identity and Access Management
36	PII security controls	Protect – Data Protection and Privacy
37	Security controls for exfiltration	Protect – Data Protection and Privacy
47	ISCM policies and strategy	Detect – ISCM
54	Incident detection and analysis	Respond – Incident Response
55	Incident handling	Respond – Incident Response
63	Testing of information system contingency plans	Recover – Contingency Planning

The weighted average is calculated by multiplying selected metrics by the priority metric weight of two and then dividing the new total for each domain. For example, the Risk Management domain has 10 metrics of which 2 are priority metrics, so the total maturity for this domain is then divided by 12 instead of 10. This same approach would be used for all domains and function areas. The overall information security program maturity rating is then an average of the function level ratings.

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 2022 Maturity Level: 4 – Managed and Measurable. OPM has policies and procedures for developing an inventory of information systems. OPM policy states that Information Security Officers (ISSO) are responsible for generating system registration forms. The registration forms are used to inventory cloud, third party, and new information systems. Public-facing websites and interconnections are inventoried as a part of the security assessment and 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. The Chief Information Security Officer (CISO) and ISSOs are held responsible for ensuring that inventory monitoring processes follow OPM's ISCM strategy. The CISO is tasked with establishing and overseeing monitoring procedures and maintaining the FISMA system inventory. The ISSO is responsible for carrying out the procedures and updating the inventory.

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

Metric 2 – Hardware Inventory

FY 2022 Maturity Level: 1 – Ad-hoc. OPM's asset management policy states that infrastructure managers must develop and document an inventory of information system components. The inventory must include specific standard data elements/taxonomy information such as manufacturer, type, model, serial number, and physical location. OPM's procedure lists the standard data elements to be used in the information system component inventory. OPM utilizes tools to capture some of the information. However, the implementation of the policy and data elements/taxonomy remains ad-hoc as they are not accompanied by other procedures that detail the process to maintain an up-to-date inventory of hardware assets with detailed information necessary for tracking and reporting. Therefore, a central hardware repository has not been established.

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

level of *Managed and Measurable*, the *Defined* maturity level must be achieved. The following recommendation is to assist OPM with attaining the *Defined* maturity level.

NIST SP 800-53, Revision 5, states that organizations with centralized inventories must "Ensure that the resulting centralized inventories include system-specific information required for proper component accountability."

Failure to maintain adequate hardware inventory elements increases the risk that system support will be adversely affected. In addition, failure to associate components of a hardware inventory with the specific information system(s) they support increases the risk that there will not be proper accountability for the component or system owner.

Recommendation 1 (Rolled forward from 2019):

We recommend that OPM define the procedures for maintaining its hardware inventory.

OPM's Response:

"Concur. OPM has defined procedures to inventory and track all hardware assets within the Remedy Asset Management Console for a subset of the agency assets. Upon receipt of hardware, the hardware is tagged with asset tags and entered in Remedy before it is entered in inventory. Before the hardware is sent to a user, it is assigned to the user in Remedy. In FY23, OPM will expand enterprise-wide hardware asset management through a recently awarded contract to build out the inventory to include all hardware components. OPM will provide the hardware inventory documentation to OIG once we have expanded the procedures to other areas."

OIG Comment:

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

Metric 3 – Software Inventory

FY 2022 Maturity Level: 1 – Ad-hoc. OPM implemented a software asset management tool in FY 2022 for end user and server systems. Separately, OPM utilizes a spreadsheet to inventory the software installed on its mainframe. Although OPM has mechanisms in place to capture some software information, policies and procedures for developing and maintaining an up-to-date software inventory have not been developed.

OPM does not have documented policies and procedures for maintaining its software inventory.

In the self-assessment OPM conducted, the goal maturity level for this metric was *Managed and Measurable*. We have assessed this metric as *Ad Hoc*. Before OPM can reach the goal maturity level of *Managed and Measurable*, the *Defined* maturity level must be achieved. The following recommendations are to assist OPM with attaining the *Defined* maturity level.

NIST SP 800-53, Revision 5, states that organizations with centralized inventories should "Ensure that the resulting inventories include system-specific information required for proper component accountability. The information necessary for effective accountability of system components includes the system name, software owners, software version numbers, hardware inventory specifications, software license information, and for networked components, the machine names and network addresses across all implemented protocols (e.g., IPv4, IPv6). Inventory specifications include date of receipt, cost, model, serial number, manufacturer, supplier information, component type, and physical location."

Failure to maintain a centralized software inventory increases the risk that the agency will not fully understand the information assets in its environment or maintain a complete major system inventory.

Recommendation 2 (Rolled forward from 2018):

We recommend that OPM define policies and procedures for a centralized software inventory.

OPM Response:

"Concur. OPM will document policies and procedures for a centralized software inventory and will provide them to OIG upon completion."

Metric 4 – System Security Categorization

FY 2022 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 states that system owners, authorizing officials and the CISO are involved with approving the security categorization of systems. OPM utilizes its Enterprise Business Impact Analysis to prioritize 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 resources, specifically ISSOs. High value asset defined system essential tasks are also assigned to ISSOs. Through these actions OPM has demonstrated that they are allocating resources through a data driven prioritization and system categorization.

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

Metric 5 – Risk Policy and Strategy

FY 2022 Maturity Level: 2 – Defined. 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. We also received evidence of a risk register and the capturing and sharing lessons learned on the effectiveness of cybersecurity risk management processes and updating the program accordingly. However, from a judgmental sample of 30 systems that we selected, 15 systems have not had a risk assessment performed in accordance with NIST guidelines and OPM's policy. OPM's risk management policy states risk assessments should be updated annually.

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

NIST SP 800-53, Revision 5, states organization should conduct a risk assessment, including, documenting risk assessment results, reviewing risk assessment results, and disseminating risk assessment results to organization defined personnel. It also states to update the risk assessment at an organization-defined frequency or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.

OPM's Risk Management Policy states that the ISSOs must, "Update the risk assessment [at least annually] or whenever there are significant changes to the information system or environment operation..."

Failure to consistently review and update risk assessments increase the risk that information systems will fail to protect sensitive information, are more vulnerable to malicious attacks, and not aligned with the agency's risk management strategy.

Recommendation 3 (Rolled forward from 2017):

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.

OPM Response:

"Concur. After the FY22 audit fieldwork concluded, OPM completed risk assessments for the IT systems. OPM will provide evidence to support closure to OIG under separate cover."

Metric 6 – Information Security Architecture

FY 2022 Maturity Level: 1 – Ad-hoc. OPM is still in the process of defining its Information Security Architecture and is instead using the Enterprise Architecture along with Cybersecurity policies, procedures, guidance and templates as a substitute. These documents and the Information System Security Plan create a 3-level tier system for Information Security Architecture. A Security Reference Model has yet to be established in the current Enterprise Architecture document. An estimated completion date of enterprise architecture has still yet to be determined by OPM.

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

NIST SP 800-53, Revision 5, defines an information security architecture as "An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational subunits, showing their alignment with the enterprise's mission and strategic plans." It also states, "The integration of security and privacy requirements and controls into the enterprise architecture helps to ensure that security and privacy considerations are addressed throughout the system development life cycle and are explicitly related to the organization's mission and business processes."

Failure to maintain an enterprise architecture with an integrated information security architecture increases the risks that the agency's security processes, systems, and personnel are not aligned with the agency mission and strategic plan.

Recommendation 4 (Rolled forward from 2017):

We recommend that OPM update its enterprise architecture, to include the information security architecture elements required by NIST and OMB guidance.

OPM Response:

"Concur. OPM recently hired a Chief Cybersecurity Architect and an Enterprise Architect who both onboarded at the end of the FY22 fiscal year who will coordinate the integration of the enterprise security architecture into the overall enterprise architecture. A project to develop the OPM Enterprise Security Reference Model is in progress."

Metric 7 – Risk Management Roles, Responsibilities, and Resources

FY 2022 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 the Enterprise Risk Management Policy and CRMS. The CRMS was developed

in accordance with the Enterprise Risk Management Policy to ensure risk management roles align with risk management strategy. Communication of the cybersecurity risk management and enterprise risk management is achieved by both polices addressing roles of the: CISO, ISSO, Authorizing Officials, System Owners, and the Risk Management Council. OPM provided ample evidence that Risk Management Council meetings occur to provide input on the cybersecurity risk register. The Risk Management Council is also responsible for advocating for an appropriate level of funding and resources to support Enterprise Risk Management and internal control functions. Evidence of performance standards were also provided by OPM, which hold Cybersecurity personnel accountable for risk management responsibilities. Cybersecurity program managers are held accountable for allocating resources and implementing risk management processes through the performance standards as well.

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

Metric 8 – Plan of Action and Milestones

FY 2022 Maturity Level: 3 – Consistently Implemented. OPM has thoroughly defined and communicated policies and procedures for the effective use of Plan of Action and Milestones (POA&M). The policies and procedures in place at OPM address: the centralized tracking of security weaknesses, prioritization of remediation efforts, maintenance, and independent validation of POA&M activities. OPM utilizes a prioritized and consistent approach to POA&Ms through the use risk assessments, security categorizations, control deficiencies, and risk ratings. Using Archer as a risk repository OPM is consistently trying to utilize POA&Ms to mitigate security weaknesses. Dashboards in Archer allow OPM to see the number of POA&Ms in various stages such as initial, draft, and Open.

The POA&Ms risk levels are categorized as Very High, High, Medium, Low or Very Low. The OPM Information Security Continuous Monitoring Metrics establish remediation timelines for vulnerabilities that include no more than 15 days for *Very High* risks, 30 days for *High* risks, 60 days for *Medium* risks, 120 days for *Low* risks, and 180 days for *Very Low* risks. However, we observed that a majority of Open POA&Ms exceed these thresholds. For example, of the 17 Open POA&Ms rated as *High*, 15 exceeded the 30 days remediation window. Of those 15, 9 exceeded by 146 days or more. For Open POA&Ms rated as *Medium*, 209 of out of 242 exceeded the 60-day remediation window. Of those 209, 126 have been Open for longer than 300 days. The OPM Information Security Continuous Monitoring Metrics has a target of 100% closure rate of Open POA&Ms by the remediation deadlines for the different risk levels, with a rating format of greater than or equal to 95% being green, greater than or equal to 80% being yellow and less than 80% being red. Less than 80% of Open POA&Ms adhere to the remediation timelines established in the Information Security Continuous Monitoring Metrics.

Although OPM has made progress in updating POA&M dates that are past due and uses dashboards in Archer, progress still needs to be made to achieve the *Managed and Measurable*

maturity level. OPM must monitor and analyze qualitative and quantitative performance measures of the effectiveness of its POA&M activities and use that information to make appropriate adjustments to ensure that its risk posture is maintained. As discussed earlier, the majority of Open POA&Ms categorized as High and Medium exceed the number of days that the POA&M should be remediated. OPM's current process for closing POA&Ms needs improvement to ensure that POA&Ms are closed in a timely manner according to their risk categorization.

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

Failure to remediate Open POA&Ms that exceed their risk categorization remediation timeline increases the risk that agency systems may be vulnerable to exploitation.

Recommendation 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.

OPM Response:

"Concur. To advance to the next FISMA maturity level of Managed and Measurable, OPM will review and update our related policies and the metric in the Information Security Continuous Monitoring Metrics document. Monitoring of this metric will be built into the current continuous monitoring dashboards in our Governance, Risk and Compliance tool and regular review will occur with our Plan of Actions and Milestones (POA&M) metrics review. We will update the POA&Ms to be manageable. After months of successful tracking, OPM will submit closure evidence to the OIG."

Metric 9 – Risk Communication

FY 2022 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. POA&Ms are documented with required criteria, defined within the POA&M Guide, as a part of the tool. ISSOs are responsible for supporting System Owners and Business Program Managers with the management of POA&Ms including communication. At an enterprise level, automated reports are also established to notify stakeholders of the POA&Ms that exist for information systems. OPM created enterprise continuous monitoring metrics around POA&Ms to support timely communication and management of cybersecurity risks. This dashboard collects real-time data from the system and is reviewed on a weekly basis.

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

Metric 10 – Centralized Enterprise-wide Risk Tool

FY 2022 Maturity Level: 3 – Consistently Implemented. 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 risks/weaknesses within OPM. The guide specifically details the process a risk goes through in the GRC tool, 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 the GRC tool, and how the tool will be used for FISMA system inventory management and security control assessments. The tool is currently serving as an automated solution across the enterprise for OPM. It also serves as a repository that stores the system inventory, along with all risk controls and remediation activities associated with a system. Furthermore, risk scores and levels are identified for systems, along with having a management dashboard.

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

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 "1 – *Ad-hoc*."**

Metric 12 – SCRM Strategy

FY 2022 Maturity Level: 1 – Ad-hoc. OPM is in the process of establishing a SCRM board to lead the agency wide activities. As such, OPM has not defined and communicated an organization wide SCRM strategy. Therefore, the default maturity level for the metric is *Ad-hoc*. SCRM was a new domain added in FY 2021 and after OPM conducted its assessment to identify goal maturity levels. The following recommendation is to assist OPM with attaining the *Defined* maturity level.

The SECURE Technology Act, enacted in December 2018, states "The head of each executive agency shall be responsible for (1) assessing the supply chain risk posed by the acquisition and

use of covered articles and avoiding, mitigating, accepting, or transferring that risk, as appropriate and consistent with the standards, guidelines, and practices identified by the Council under section 1323(a)(1); and (2) prioritizing supply chain risk assessments conducted under paragraph (1) based on the criticality of the mission, system, component, service, or asset."

NIST SP 800-161 outlines how to incorporate SCRM into an agency risk management process. This includes adjusting the security controls that the agency has implemented. "The [information and communications technology] SCRM controls defined in this chapter should be selected and tailored according to individual organization needs and environment using the guidance in [NIST SP 800-53, Revision 4], in order to ensure a cost-effective, risk-based approach to providing [Information and Communication Technology] SCRM organization-wide." It also adds a family of controls "Provenance . . . developed specifically to address [information and communications technology] supply chain concerns."

Failure to assess supply chain risks increases the risk that OPM will not be able to procure the necessary resources in an effective and security conscious manner, which could result in a malicious vulnerability being introduced into the agency's technical environment.

Recommendation 6 (Rolled forward from 2019):

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.

OPM Response:

"Concur. OPM is taking steps to address Supply Chain Risk Management (SCRM) requirements. The Investment Review Board (IRB) has reviewed and provided comments to the draft charter to identify the body that will be responsible for SCRM processes and activities."

Metric 13– SCRM Policies and Procedures

FY 2022 Maturity Level: 1 – Ad-hoc. OPM is in the process of establishing a SCRM board to lead the agency wide activities. Therefore, the default maturity level for the metric is *Ad-hoc*. A recommendation in metric 12 has been issued to assist OPM with attaining the *Defined* maturity level for this metric.

Metric 14 – Adherence to Cybersecurity and Supply Chain Requirements

FY 2022 Maturity Level: 1 – Ad-hoc. OPM is in the process of establishing a SCRM board to lead the agency wide activities. Therefore, the default maturity level for the metric is *Ad-hoc*. A recommendation in metric 12 above has been issued to assist OPM with attaining the *Defined* maturity level for this metric.

Metric 15 – Component Authenticity

FY 2022 Maturity Level: 1 – Ad-hoc. OPM is in the process of establishing a SCRM board to lead the agency wide activities. Therefore, the default maturity level for the metric is *Ad-hoc*. A recommendation in metric 12 above has been issued to assist OPM with attaining the *Defined* maturity level for this metric.

Metric 16 – SCRM Additional Information

We have no additional comments regarding SCRM.

D. Configuration Management

Configuration Management (CM) 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 2022 Maturity Level: 2 – Defined. Through policies and procedures, OPM can demonstrate that individual roles and responsibilities for CM stakeholders are defined across the organization. However, an appropriate gap analysis has not been performed in order for OPM to adequately determine if individuals are consistently performing roles and responsibilities, and that the OCIO can demonstrate the resource needs of the configuration management program.

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

NIST SP 800-128 states that "For organizations with varied and complex enterprise architecture, implementing [CM] in a consistent and uniform manner across the organization requires organization-wide coordination of resources."

Failure to determine if the organization has adequate resources to manage CM operations increases the risk of improperly configured devices on the network, and an increased threat of malicious attacks.

Recommendation 7 (Rolled forward from 2017):

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.

OPM Response:

"Concur. OCIO awarded a contract that started in FY 22 to develop and document our enterprise baseline configurations for end user devices, servers, and cloud systems. OPM will submit CM evidence to the OIG under separate cover."

Metric 18 – Configuration Management Plan

FY 2022 Maturity Level: 2 – Defined. OPM has developed a CM plan that outlines CM-related roles and responsibilities, institutes a change control board, and defines 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.

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

NIST SP 800-128 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."

Failure to document lessons learned increases the risk that the configuration management process will not effectively manage the system security settings that protect the OPM environment.

Recommendation 8 (Rolled forward from 2017):

We recommend that OPM document the lessons learned from its configuration management activities and update its configuration management plan as appropriate.

OPM Response:

"Concur. OCIO awarded a contract in FY22 to develop and document our enterprise baseline configurations for end user devices, servers, and cloud systems. The configuration management program now includes those configurations. OPM will submit the evidence to the OIG under separate cover."

Metric 19 – Baseline Configurations

OPM has not developed a baseline configuration for all of its information systems.

FY 2022 Maturity Level: 1 – Ad-hoc. In FY 2022, OPM has implemented a process to migrate information systems to a cloud environment, where the cloud service provider will be responsible for developing and implementing baseline configurations. However, not all systems have migrated at this time. With the migration effort aside, OPM still has not developed baseline configurations and a component inventory for each information system. OPM has an Open recommendation in metric 2 to address the lack of hardware inventory.

OPM routinely runs automated compliance scans on its information systems to ensure that no system configurations are modified outside of the approved change control process. However, OPM does not currently run routine baseline configuration checks to verify that information systems are in compliance with pre-established baseline configurations, as they have yet to be developed.

In the self-assessment OPM conducted, the goal maturity level for this metric was *Consistently Implemented*. We have assessed this metric as *Ad-hoc*. Before OPM can reach the goal maturity level of *Consistently Implemented*, the *Defined* maturity level must be achieved. The following recommendation is to assist OPM with attaining the *Defined* maturity level.

NIST SP 800-53, Revision 5, states that "Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture."

NIST SP 800-53, Revision 5, states that the organization should "Develop, document, and maintain under configuration control, a current baseline configuration of the system…."

Failure to document a baseline configuration increases the risk that devices within the network are not configured in accordance with agency policies and leaves them vulnerable to malicious attacks that exploit those misconfigurations.

Recommendation 9 (Rolled forward from 2017):

We recommend that OPM develop and implement a baseline configuration for all information systems in use by OPM.

OPM Response:

"Concur. OPM is identifying and documenting modern baseline configurations based on the current Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). We have configuration settings for recent implementations. The agency will continue documenting, testing, and implementing the exceptions and variations to the baselines."

Metric 20 – Security Configuration Settings

FY 2022 Maturity Level: 1 – Ad-Hoc. OPM has a project plan in development to address its configuration settings and common secure configurations. However, the project plan has not been implemented and the process for establishing policies and procedures that would establish configuration settings and common secure configurations has not been defined, implemented, or monitored.

In the self-assessment OPM conducted, the goal maturity level for this metric was *Defined*. We have assessed this metric as *Ad-hoc*. The following recommendations are to assist OPM with attaining the *Defined* maturity level.

NIST SP 800-53, Revision 5, states the organization should establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using organization-defined common secure configurations.

Failure to document security configuration settings for all information systems increases the risk of insecurely configured systems.

Recommendation 10 (Rolled forward from 2014):

We recommend that the OCIO develop and implement standard security configuration settings for all operating platforms in use by OPM.

OPM Response:

"Concur. OPM is identifying and documenting modern baseline configurations for the agency based on the current DISA STIGs. We patched legacy systems to update the standard security configuration settings. We will continue documenting, testing, and implementing the exceptions and variations to the baselines incorporating standard security configuration settings."

Recommendation 11 (Rolled forward from 2016):

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.

OPM Response:

"Concur. OPM has identified and documented all exceptions to the DISA STIGs baseline configurations for the agency end user devices. The agency will continue documenting, testing, and implementing the exceptions and variations to the baselines. OPM will submit the evidence to the OIG under separate cover."

Metric 21 – Flaw Remediation and Patch Management

FY 2022 Maturity Level: 2 – Defined. In FY 2022, OPM provided an up-to-date Patch Management Policy, and Configuration Management Policies and Procedures. Although our testing did not identify any critical vulnerabilities that were not remediated within 30 days of the patch release for the distributed systems, we did identified vulnerabilities that exceeded 30 days for the mainframe.

We also determined that there is no formal process in place to ensure that all new devices on the agency's network are included in the scanning process.

In the self-assessment OPM conducted, the goal maturity level for this metric was *Consistently Implemented*. We have assessed this metric as *Defined*. The following recommendations are 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 "within [30 days] of 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 of 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 12 (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 Response:

"Concur. As outlined in OPM's policy and procedures, POA&Ms are created for patches exceeding the mandated timeframe. Risk acceptances could be issued for patches that are managed through mitigating controls. We are updating our IT security policies and procedures to meet National Institute of Standards and Technology (NIST) Special

Publication (SP) 800-53 Revision 5. OPM will also review and update the patching procedures as necessary. Once finalized, OPM will provide the updated documentation to OIG."

Recommendation 13 (Rolled forward from 2018):

We recommend that the OCIO implement a process to ensure new server installations are included in the scan repository.

OPM Response:

"Concur. OPM is adjusting processes related to our Network Access Control (NAC) and scanning tool to incorporate automation and to improve performance."

Metric 22 – Trusted Internet Connection Program

FY 2022 Maturity Level: 1 – Ad-hoc. In FY 2022, OPM did not provide any evidence to demonstrate that the Trusted Internet Connection (TIC) controls meet the defined or consistently implemented levels for this metric.

In the self-assessment OPM conducted, the goal maturity level for this metric was *Consistently Implemented*. We have assessed this metric as *Ad-hoc*. Before OPM can reach the goal maturity level of *Consistently Implemented*, the *Defined* maturity level must be achieved. The following recommendation 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."

Without a formal process TIC program OPM cannot maintain the high level of security needed to protect networks from malicious actors.

Recommendation 14 (Rolled forward from 2021):

We recommend that OPM establish an agency-wide TIC program to manage and maintain its external agency connections.

OPM Response:

"Concur. OPM has built and implemented a Trusted Internet Connection (TIC) program over the last few years. OPM has provided OIG the capabilities and infrastructure required to participate in the TIC, Einstein and Continuous Diagnostics and Mitigation (CDM) programs. OPM has also met the Federal TIC security requirements. OPM will improve our documentation and communication of our TIC environment and will gather the required

documentation for follow-up with the respective Federal authorities."

Metric 23 – Configuration Change Control Management

FY 2022 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, the goal maturity level for this metric was *Consistently Implemented*. We have assessed this metric as *Consistently Implemented*.

Metric 24 - Vulnerability Disclosure Policy

FY 2022 Maturity Level: 2 – Defined. OPM has a vulnerability disclosure policy 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.

This is a new metric that was added in FY 2021 after OPM conducted its self-assessment to identify goal maturity levels. We have assessed this metric as *Defined*. We will reassess this metric in next year's FISMA audit.

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 (FICAM) 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 "2 – *Defined*."**

Metric 26 – ICAM Roles, Responsibilities, and Resources

OPM has not developed a comprehensive ICAM strategy.

FY 2022 Maturity Level: 1 – Ad Hoc. OPM has individual policies and procedures that define roles and responsibilities for specific aspects of ICAM. However, OPM has not developed an ICAM governance structure to align and consolidate the agency's ICAM investments, monitor programs, and ensure awareness and understanding. Roles and responsibilities for all users should be incorporated in a comprehensive ICAM strategy. However, OPM is still in the process of creating a charter for the ICAM governance structure and a comprehensive ICAM strategy.

In the self-assessment OPM conducted, the goal maturity level for this metric was *Managed and Measurable*. We have assessed this metric as *Ad-hoc*. Before OPM can reach the goal maturity level of *Managed and Measurable*, the *Defined* maturity level must be achieved. The following recommendation is to assist OPM with attaining the *Defined* maturity level.

OMB Memorandum M-19-17 states that "Each agency shall designate an integrated agency-wide ICAM office, team, or other governance structure in support of its Enterprise Risk Management capability to effectively govern and enforce ICAM efforts." The FICAM Playbook for Program Governance and Leadership recommends that the agency create a charter to govern the roles and responsibilities of its governance body.

Failure to establish an agency wide ICAM governance structure negatively impacts OPM's ability to coordinate the ICAM program and provide effective oversight.

Recommendation 15 (Rolled forward from FY 2021):

We recommend that OPM create a charter to govern the roles and responsibilities of its ICAM office's governance body.

OPM Response:

"Concur. The draft OPM Identity, Credential and Access Management (ICAM) governance charter is routing for internal concurrence. OPM will provide the documentation to OIG once it is final."

Metric 27 – ICAM Strategy

FY 2022 Maturity Level: 1 – Ad-Hoc. OPM has not developed a comprehensive ICAM strategy to guide its ICAM processes and activities. Before OPM can develop a comprehensive ICAM strategy, it must create milestones for how it plans to align with Federal initiatives including strong authentication, the Federal ICAM architecture and OMB M-19-17, and phase 2 of DHS's Continuous Diagnostics and Mitigation (CDM) program, as appropriate. These milestones

should be incorporated in an ICAM transition roadmap which defines how OPM plans to achieve the desired state of its ICAM strategy. However, OPM has not developed these milestones.

In the self-assessment OPM conducted, the goal maturity level for this metric was *Consistently Implemented*. We have assessed this metric as *Ad-hoc*. Before OPM can reach the goal maturity level of *Consistently Implemented*, the *Defined* maturity level must be achieved. The following recommendation is to assist OPM with attaining the *Defined* 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 FICAM Roadmap and Implementation Guidance states that "Agencies are to align their relevant segment and solution architectures to the common framework defined in the government-wide ICAM segment architecture. Alignment activities include a review of current business practices, identification of gaps in the architecture, and development of a transition plan to fill the identified gaps."

The absence of an ICAM strategy that includes a review of current practices, identification of gaps, and a transition plan increases the risk that OPM will not successfully the Federal ICAM initiatives.

Recommendation 16 (Rolled forward from FY 2017):

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.

OPM Response:

"Concur. OPM's draft ICAM strategy is routing for internal concurrence. OPM will provide the documentation to OIG once it is final."

Metric 28 – Personnel Risk

FY 2022 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, the goal maturity level for this metric was *Consistently Implemented*. We have assessed this metric as *Consistently Implemented*.

Metric 29 – Access Agreements

FY 2022 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 access agreements prior to being granted access to systems and are maintained on an annual basis thereafter, as a part of IT Security and Privacy Awareness training.

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

Metric 30 – Multi-factor Authentication with Personal Identity Verification (PIV)

FY 2022 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, the goal maturity level for this metric was *Consistently Implemented*. We have assessed this metric as *Consistently Implemented*.

Metric 31 – Strong Authentication Mechanisms for Privileged Users

FY 2022 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, the goal maturity level for this metric was *Consistently Implemented*. We have assessed this metric as *Consistently Implemented*.

Metric 32 – Management of Privileged User Accounts

FY 2022 Maturity Level: 1 – Ad-hoc. OPM has defined its process for provisioning and deprovisioning non-privileged accounts. However, OPM has not defined its process for provisioning, managing, and reviewing privileged accounts. Defined processes should cover approval, tracking, inventorying, validating, logging, and reviewing privileged users' accounts. OPM provided evidence of documented requests and approvals for privileged account access. However, the process has not been formally defined and documented.

In the self-assessment OPM conducted, the goal maturity level for this metric was *Managed and Measurable*. We have assessed this metric as *Ad-hoc*. Before OPM can reach the goal maturity level of *Managed and Measurable*, the *Defined* maturity level must be achieved. The following recommendation is to assist OPM with attaining the *Defined* maturity level.

NIST SP 800-53, Revision 5, states that the organization develops and documents "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 17 (Rolled forward from 2021):

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

OPM Response:

"Concur. OPM has a documented process to create, manage, and review privileged accounts. Requests for privileged accounts are submitted by a Federal Manager using a Privileged Account Request Form. Each request is reviewed and signed off by Enterprise Infrastructure Services (EIS) management. EIS Operations administrators approve and manage privileged accounts. OPM run automated reports bi-monthly to show privileged account permissions and user disablement. OPM sent the supporting documentation to OIG after the audit fieldwork concluded."

Metric 33 – Remote Access Connections

FY 2022 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. However, OPM did not provide evidence demonstrating that it has established and documented configuration and connection requirements which must be met prior to authorizing remote access. OPM has implemented a reactive solution which scans for misconfigured hosts, but this occurs after the host has already established a remote connection and has been granted access to the internal network.

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

NIST SP 800-53, Revision 5, states that the organization should "Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and Authorize each type of remote access to the system prior to allowing such connections."

Failure to ensure that end user devices are appropriately configured prior to authorizing remote access, increases the risk that vulnerable or compromised devices will be allowed on the network.

Recommendation 18:

We recommend that OPM establish and document configuration and connection requirements which must be met prior to authorizing remote access.

OPM Response:

"Concur. OPM is implementing Zero Trust principals to address this recommendation."

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 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 2022 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 Personally Identifiable Information (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.

Although the privacy program has been established, additional steps need to be taken to ensure the program is consistently implemented. These steps include dedicating appropriate resources to the privacy program and ensuring that individuals are consistently performing the privacy roles and responsibilities that have been defined across OPM. OPIM stated that staffing and resource needs have been identified and OPIM is in the process of hiring additional privacy staff.

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

OMB 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 19:

We recommend that OPM acquire the identified resources for the privacy program.

OPM Response:

“Concur. The Office of Privacy and Information Management (OPIM) prepared a staffing plan for Fiscal Year 2023 for review by OPM’s Human Resources and Strategic Hiring Committee to identify specific positions that OPIM intends to hire in FY23 to build the privacy program. OPIM will proceed with our hiring actions once the plan is approved.”

Recommendation 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.

OPM Response:

“Partially Concur. We do not concur with the recommendation insofar as it states that we do not currently have processes in place to ensure consistent performance of privacy roles and responsibilities. Within OPIM, the privacy analysts and other staff have clearly defined position descriptions, and annual performance plans that are reviewed regularly. In addition, OPIM works closely with the OCIO Cybersecurity staff and program offices to address privacy compliance requirements related to the Authorization to Operate process, to include their role in completing Privacy Threshold Analyses and Privacy Impact Assessments, as necessary. We concur with the recommendation insofar as we recognize that there are additional steps that we can take to establish more consistency across OPM and we will look for opportunities going forward, subject to other priorities and resource constraints.”

OIG Comment:

During audit fieldwork, we did not receive the aforementioned annual performance plans or any evidence demonstrating that a process is in place to ensure the consistent performance of privacy roles and responsibilities. If OPIM has implemented the recommendation, then as part of the audit resolution process, we recommend that the OPIM provide IOC with evidence that the agency implemented this recommendation.

Metric 36 – Data Protection and Privacy Controls

FY 2022 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 that OPM conducted, the goal maturity level for this metric was *Consistently Implemented*. We have assessed this metric as *Consistently Implemented*.

Metric 37 – Data Exfiltration Prevention

FY 2022 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, the goal maturity level for this metric was *Managed and Measurable*. We have assessed this metric as *Managed and Measurable*.

Metric 38 – Data Breach Response Plan

FY 2022 Maturity Level: 2 – Defined. OPM has defined and communicated its Data Breach Response Plan, including its processes and procedures for data breach notification. As a part of the plan, a Breach Response Team has been established that includes the appropriate agency officials. OPM's breach response plan requires periodic testing and updating. However, similar to last year, OPM has not updated or tested its Data Breach Response Plan this year.

OPM has not updated or tested its Data Breach Response Plan.

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

OPM's Breach Response Plan states that "The [Senior Agency Official for Privacy] must periodically convene OPM's [Breach Response Team] to hold a tabletop exercise. The purpose of the tabletop exercise is to test the [Breach Response Plan] and to help ensure that members of the [Breach Response Team] are familiar with the plan and understand their specific roles. Testing the [Breach Response Plan] is an essential part of risk management and breach response preparation. Tabletop exercises should be used to practice a coordinated response to a breach, to

further refine and validate the breach response plan, and to identify potential weaknesses in OPM's response capabilities."

NIST SP 800-122, states that "The policies and procedures should be communicated to the organization's entire staff through training and awareness programs. Training may include tabletop exercises to simulate an incident and test whether the response plan is effective and whether the staff members understand and are able to perform their roles effectively."

Failure to routinely test the Data Breach Response Plan increases OPM's risk of major data loss in the event of a security incident. Testing the plan increases the likelihood that a breach response will be efficient and effective at limiting the affects from a security incident.

Recommendation 21 (Rolled forward from 2018):

We recommend that OPM develop a process to routinely test the Data Breach Response Plan.

OPM Response:

"Concur. The existing Breach Response Plan was issued in 2017. OPIM plans to update the plan, including developing an annual table-top exercise, as resources permit. OPIM and OCIO will also coordinate all table-top exercises."

Metric 39 – Privacy Awareness Training

FY 2022 Maturity Level: 1 – Ad-Hoc. OPM reviews and updates the annual Cybersecurity and Privacy training. Although OPIM stated that they have identified individuals with heightened responsibility for PII and have provided role-based training to supervisors, we did not receive any evidence to support that claim. Identifying individuals would include formal documentation. Additionally, OPIM plans to formalize role-based privacy training for individuals having responsibility for PII or activities involving PII.

In the self-assessment OPM conducted, the goal maturity level for this metric was *Consistently Implemented*. We have assessed this metric as *Ad-hoc*. Before OPM can reach the goal maturity level of *Consistently Implemented*, the *Defined* maturity level must be achieved. The following recommendation is to assist OPM with attaining the *Defined* maturity level.

OMB Memorandum 17-12 states that "Agencies should not limit training on how to identify, report, and respond to a suspected or confirmed breach to annual security and privacy training. Rather, agencies should consider annual security and privacy training as the baseline and consider specialized training for specific groups, such as supervisors and employees who have access to or responsibility for High Value Assets."

OMB Circular A-130 requires agencies to "Provide foundational as well as more advanced levels of security and privacy training to information system users (including managers, senior

executives, and contractors) and ensure that measures are in place to test the knowledge level of information system users;" and to "Provide role-based security and privacy training to employees and contractors with assigned security and privacy roles and responsibilities, including managers, before authorizing access to Federal information or information systems or performing assigned duties... ."

OPM policy requires users to "Complete role-based security or privacy training if assigned a significant security or privacy role" and system owners to "Provide role-based security and privacy training to OPM information system users responsible for the operation of security functions/mechanisms for systems under his or her portfolio."

NIST SP 800-122 states that "To reduce the possibility that PII will be accessed, used, or disclosed inappropriately, all individuals that have been granted access to PII should receive appropriate training and, where applicable, specific role-based training."

Failure to provide specific training to individuals with assigned security and privacy roles and responsibilities increases OPM's risk of improperly implemented controls, which can lead to mishandled data resulting in a data loss incident.

Recommendation 22 (Rolled forward from 2018):

We recommend that OPM identify individuals with heightened responsibility for PII and provide role-based training to these individuals at least annually.

OPM Response:

"Partially Concur. We do not concur with the recommendation to the extent it states that we have not previously identified individuals with heightened responsibility for Personal Identifiable Information (PII) and provided them with training. The OPIM has provided training in the past to supervisors, senior leadership, and other offices, such as the Office of the Chief Financial Officer, with significant responsibility for PII. We partially concur that it would be beneficial to formally document those for whom role-based training would be beneficial for the agency and to provide such training more systematically."

OIG Comment:

During audit fieldwork, we did not receive evidence that individuals with heightened responsibility for PII were identified nor evidence of any training provided to them. If OPIM has implemented the recommendation, then as part of the audit resolution process, we recommend that the OPIM provide IOC with evidence that the agency implemented this recommendation.

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 2022 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, the goal maturity level for this metric was *Consistently Implemented*. We have assessed this metric as *Consistently Implemented*.

Metric 42 – Assessment of Workforce

FY 2022 Maturity Level: 3 – Consistently Implemented. OPM has tailored its awareness and specialized training needs and has preliminarily identified the skill gaps for the agency's cybersecurity workforce. While OPM has obtained and hired ISSO support, it is our understanding OPM will continue to assess the workforce to address future needs of the agency. Additionally, although obtaining ISSO support does demonstrate progress in this area that allows OPM to be *Consistently Implemented*, an updated gap analysis to determine any weaknesses and specialized training needs will need to continue as OPM's workforce evolves.

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

Metric 43 – Security Awareness Strategy

FY 2022 Maturity Level: 3 – Consistently Implemented. In FY 2022, the security awareness and training strategy has been fully developed and consistently implemented to maintain a security awareness program tailored to the mission and risk environment. OPM also continues to conduct gap analyses and periodic re-assessments of organizational skills.

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

Metric 44 – Tracking IT Security Training

FY 2022 Maturity Level: 4 – Managed and Measurable. The OCIO provides annual IT security and privacy awareness training to all OPM users through an interactive web-based course. The course introduces employees and contractors to the basic concepts of IT security and privacy, including topics such as the importance of information security, security threats and vulnerabilities, privacy training, telework, mobile devices, Wi-Fi guidance, and the roles and responsibilities of users. In addition, OPM conducts random phishing exercises and tracks the results to measure the effectiveness of the exercises. OPM also conducts associated follow-ups, and these are used to update the IT security training program. All OPM's employees and contractors completed the security awareness training course in FY 2022.

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

Metric 45 – Tracking Specialized IT Security Training

FY 2022 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, the goal maturity level for this metric was Managed and Measurable. We have assessed 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

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 "2 – *Defined*."**

Metric 47 – ISCM Policies Strategy

FY 2022 Maturity Level: 2 – Defined. OPM has developed ISCM strategies that addresses the monitoring of security controls at the organization, business unit, and individual information

system levels. At the organization and business unit levels, the ISCM strategies define how OPM's activities support risk management in accordance with organizational risk tolerance. At the information system level, the ISCM program has establishes processes for monitoring security controls for effectiveness and reporting any findings. OPM has also developed ISCM policies tailored to OPM's environment including specific requirements and deliverables.

In the self-assessment OPM conducted, the goal maturity level for this metric was *Consistently Implemented*. We have assessed the maturity level of this metric as *Defined*. To achieve the *Consistently Implemented* maturity level for this metric, OPM's ISCM policies and strategy need to be consistently implemented at the organization, business process and information system levels. As we will discuss in metric 49, OPM's Security Assessment and Authorization process and testing of security controls are not consistently implemented. Since metric 49 is not *Consistently Implemented*, OPM's ISCM strategy and policies cannot achieve the *Consistently Implemented* maturity level. Therefore, a recommendation will not be issued for this metric.

Metric 48 – ISCM Roles, Responsibilities, and Resources

FY 2022 Maturity Level: 2 – Defined. OPM has defined the structure, roles, and responsibilities of its ISCM teams and stakeholders. However, OPM has not ensured that individuals are consistently performing the defined ISCM roles and responsibilities.

In the self-assessment OPM conducted, the goal maturity level for this metric was *Consistently Implemented*. We have assessed the maturity level of this metric as *Defined*. To achieve the *Consistently Implemented* maturity level for this metric, OPM should ensure that individuals are performing the roles and responsibilities that have been defined across the organization. As we will discuss in metric 49, OPM's Security Assessment and Authorization process and testing of security controls are not consistently implemented. Since metric 49 is not *Consistently Implemented*, the individual performance of all the defined roles and responsibilities cannot achieve the *Consistently Implemented* maturity level. Therefore, a recommendation will not be issued for this metric.

Metric 49 – Ongoing Security Assessments

FY 2022 Maturity Level: 2 – Defined. OPM has defined its processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls for individual systems. However, OPM's Security Assessment and Authorization (Authorization) process and testing of security controls are not consistently implemented.

OPM is not conducting quarterly testing on all systems.

1) Controls Testing

   We found that many systems are not following the security control-testing schedule that the OCIO has mandated for all systems. OPM policy requires reporting the security status of

information systems to the CIO for the organization and Authorizing Official for the systems at least quarterly.

We reviewed evidence of security control testing for the first two quarters of FY 2022 for all 48 of OPM's major systems. Of those, 45 systems were subject to security controls testing that complied with OPM's requirements for the first quarter. However, only 21 systems were subject to security control testing for the second quarter. OPM is not conducting quarterly testing on all systems.

2) System Authorizations

Of the 48 system Authorizations we reviewed, 19 were signed by agency officials no longer the Authorizing Official, a situation that necessitates re-authorization by the new Authorizing Official as stated in NIST SP 800-37, Revision 1.

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

Metric 50 – Measuring ISCM Program Effectiveness

FY 2022 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, the goal maturity level for this metric was *Consistently Implemented*. We have assessed 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 reacting 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 2022 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 the goal maturity level of *Managed and Measurable*. We have assessed this metric as *Managed and Measurable*.

Metric 53 – Incident Roles and Responsibilities

FY 2022 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, the goal maturity level for this metric was *Managed and Measurable*. We have assessed this metric as *Managed and Measurable*.

Metric 54 – Incident Detection and Analysis

FY 2022 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, the goal maturity level for this metric was *Managed and Measurable*. We have assessed this metric as *Managed and Measurable*.

Metric 55 – Incident Handling

FY 2022 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, the goal maturity level for this metric was *Managed and Measurable*. We have assessed this metric as *Managed and Measurable*.

Metric 56 – Sharing Incident Response Information

FY 2022 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. There are controls 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, the goal maturity level for this metric was *Managed and Measurable*. We have assessed this metric as *Managed and Measurable*.

Metric 57 – Contractual Relationships in Support of Incident Response

FY 2022 Maturity Level: 4 – Managed and Measurable. OPM collaborates with DHS and other parties, when needed, for technical assistance, surge resources, and any special requirements to quickly respond 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, the goal maturity level for this metric was *Managed and Measurable*. We have assessed this metric as *Managed and Measurable*.

Metric 58 – Technology to Support Incident Response

FY 2022 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, the goal maturity level for this metric was *Managed and Measurable*. We have assessed 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 "2 – *Defined*."**

Metric 60 – Contingency Planning Roles and Responsibilities

FY 2022 Maturity Level: 2 – Defined. 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.

While OPM is making progress, we continue to see that roles and responsibilities related to contingency plan maintenance and testing are not being consistently performed. To address gaps related to contingency planning activities, OPM has reevaluated roles and responsibilities which will be communicated during an upcoming Investment Review Board meeting and agency wide FISMA briefing. The objective of the Investment Review Board's meeting is to clarify the role, responsibilities, expectations related to OCIO's involvement in support of the systems' operation.

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

NIST SP 800-34, Revision 1, states that, "Recovery personnel should be assigned to . . . teams that will respond to the event, recover capabilities, and return the system to normal operations."

Failure to staff critical roles in the contingency planning process increases the risk that OPM will be unable to restore systems to an operational status in the event of a disaster.

Recommendation 23 (Rolled forward from FY 2018):

We recommend that OPM perform a gap-analysis to determine the contingency planning requirements (people, processes, and technology) necessary to implement the agency's contingency planning policy effectively.

OPM Response:

"Concur. OPM will further incorporate contingency planning roles and requirements details into the appropriate training programs. We will target System Owners, Authorizing Officials, and OCIO staff. Evidence of this role clarification and training will be provided OIG."

Metric 61 – Business Impact Analysis

FY 2022 Maturity Level: 2 – Defined. 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 has created a BIA worksheet template. However, the BIA Worksheet template does not include all the requirements stated in NIST SP 800-34, Revision 1. Those requirements are: determine mission/business processes and recovery criticality; identify resource requirements; and identify recovery priorities for system resources. We performed control tests on a randomly selected sample of 5 BIAs to determine whether all criteria outlined in NIST SP 800-34, Revision 1, were documented. None of the BIAs include all of the requirements. BIAs for 45 of the 48 systems included in the FISMA inventory use the OPM BIA Worksheet template which does not incorporate all NIST SP 800-34, Revision 1, BIA requirements.

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

NIST 800-34, Revision 1, states that three steps are typically involved in accomplishing the BIA: determine mission/business processes and recovery criticality; identify resource requirements; and identify recovery priorities for system resources.

Failure to document all data required to perform a BIA increases the risk that the agency will be unable to prioritize recovery operations effectively and efficiently, in the event of a service impacting incident.

Recommendation 24:

We recommend that OPM update the BIA Worksheet template to include all criteria outlined in NIST SP 800-34, Revision 1.

OPM Response:

"Partially Concur. OPM consistently reviews and implements the required criteria from SP 800-34 Rev. 1. We will conduct a thorough review of the current Business Impact Analysis (BIA) Worksheet template against NIST SP 800-34, Rev. 1 during the evaluation of information systems and operations as part of contingency planning requirements and priorities planning. As a result of our review of the template against the Special Publication, OPM will document the deltas in a gap analysis. We will update the templates, as necessary and will provide the templates and gap analysis to OIG."

OIG Comment:

During the audit, we identified and listed in the report several requirements from NIST SP 800-34, Revision 1, that were not in the BIA template. If OPM has implemented the recommendation, then as part of the audit resolution process, we recommend that the OPIM provide IOC with evidence that the agency implemented this recommendation.

Metric 62 – Contingency Plan Maintenance

FY 2022 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 5 out of 48 of its systems. Existing information system contingency plans have not been reviewed and updated within the last year for 15 out of 48 systems tested as required by OPM policy.

In an effort to ensure that contingency planning roles and responsibilities are being consistently performed, the OCIO Contingency of Operations Planning Manager is interacting with personnel responsible for executing the development of OCIO Contingency of Operations plans and standard operating procedures. Additionally, the OCIO Contingency of Operations Planning Manager regularly communicates the status of Contingency of Operations Planning activities to the Contingency Working Group and Director of Emergency Management.

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

NIST SP 800-34, 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 increase the risk that the agency will be unable to restore operations effectively and efficiently in the event of a service impacting incident.

Recommendation 25 (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 Response:

"Concur. As part of current OPM Security Authorization Guide and Risk Management Framework (RMF) process, a Contingency Plan (CP) is a required element of all major systems to obtain an authorization to operate. OPM will ensure that the contingency plans are reviewed and updated as part of the plan testing process."

Metric 63 – Contingency Plan Testing

OPM has not effectively performed annual contingency plan testing for all systems within its inventory.

FY 2022 Maturity Level: 1 – Ad-hoc. Developing a sufficient plan for an information system contingency test and routinely performing it is a critical step in ensuring plans can be executed successfully in the event of a disaster. The Contingency Planning Manager is responsible for developing the plan for the information system contingency test and overseeing the execution of that test. As in last year, OPM has not effectively performed annual contingency plan testing for all systems within its inventory since 2008. OPM has not tested 24 out of 48 information system contingency plans within the last year. Additionally, it has been identified that contingency planning policies and procedures define some, but not all, test areas required to be considered sufficient. The missing requirements include notification procedures; system recovery on an alternate platform from backup media; internal and external connectivity; system performance using alternate equipment; restoration of normal operations and other plan testing where coordination is identified

In the self-assessment OPM conducted, the goal maturity level for this metric was *Consistently Implemented*. We have assessed this metric as *Ad-Hoc*. Before OPM can reach the goal maturity level of *Consistently Implemented*, the *Defined* maturity level must be achieved. The following recommendations are to assist OPM with attaining the *Defined* maturity level.

NIST SP 800-34, Revision 1, states that "The following areas should be addressed in a contingency plan test, as applicable: notification procedures; system recovery on an alternate platform from backup media; internal and external connectivity; system performance using alternate equipment; restoration of normal operations; and other plan testing where coordination is identified."

NIST SP 800-53, Revision 5, states that an organization should 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 service impacting incident.

Recommendation 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.

OPM Response:

"Concur. While agencies are required to follow NIST guidance in accordance with Office of Management and Budget (OMB) policy, there is flexibility within NIST's guidance in how agencies apply the guidance. Unless otherwise specified by OMB, the 800-series guidance generally allows agencies some latitude in the application. OPM has consistently reviewed and implemented the required criteria from SP 800-34 Rev 1 into the Contingency Plan development. As indicated in previous system level audits, OPM is compliant with 800-34 Rev 1 criteria.

OPM will take the required steps to ensure that the required areas of NIST SP 800-34 Rev. 1 are considered within related policies and procedures to test the contingency plans."

Recommendation 27 (Rolled forward from 2008):

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

OPM Response:

"Concur. We are developing (when necessary) and executing POA&Ms with system owners and supported Office Heads to test the contingency plans for each system on an annual basis."

Metric 64 – Information System Backup and Storage

FY 2022 Maturity Level: 1 – Ad-Hoc. OPM policy defines controls for data backup, recovery, and testing. However, OPM did not provide evidence that alternative approaches were considered when developing its backup and storage strategies, including cost, environment, maximum downtimes, recovery priorities, and integration with other contingency plans. OPM did not respond to a request for further information.

Additionally, OPM did not provide evidence demonstrating that has implemented a past recommendation to ensure security safeguards for alternate processing and storage sites are equivalent to the primary sites. OPM stated that it is in the process of migrating from legacy datacenters to cloud infrastructure and has carefully assessed the security mechanisms associated with the cloud environment. However, we did not receive evidence of this assessment. Furthermore, this assessment does not describe how these controls are implemented at the time of this audit.

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

maturity level of *Consistently Implemented*, the *Defined* maturity level must be achieved. The following recommendations are to assist OPM with attaining the *Defined* maturity level.

NIST SP 800-34, Revision 1, states that "several alternative approaches should be considered when developing and comparing strategies, including cost, maximum downtimes, security, recovery priorities, and integration with larger, organization-level contingency plans."

NIST SP 800-53, Revision 5, states that an organization should "Provide controls at the alternate processing site that are equivalent to those at the primary site."

Without testing and assurance of equivalent information security safeguards at alternate storage and processing sites, there is an increased risk that data will be compromised or lost during system recovery activities.

Failure to consider alternative approaches for back up and storage strategies increases the risk that the strategy selected will not meet the availability requirements of the system.

Recommendation 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.

OPM Response:

"Concur. As OPM implements the Cloud First Strategy, we will take every opportunity to use cloud technology and FedRAMP cloud service providers. OPM is taking steps to reduce the number of cloud environments within OPM. For example, we recently transitioned our Enterprise Cost Accounting System (ECAS) to OPM's Enterprise Cloud from a third-party cloud provider. Regarding cloud backup and storage, we are evaluating and documenting available cloud data management, file system, and storage solutions. We are also evaluating and documenting the dependencies for storage scenarios and requirements. We will continually take advantage of the native cloud capabilities and features including disaster recovery and high availability. OPM will provide the documentation to OIG once it is final."

Recommendation 29 (Rolled forward from 2020):

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.

OPM Response:

"Concur. OPM will document security controls equivalent to the primary sites and test them through the system level assessment process, as part of the related risk management framework's phase to adequately meet the required safeguards. As we implement the Cloud

First Strategy, we will take every opportunity to use cloud technology and FedRAMP cloud service providers."

Metric 65 – Communication of Recovery Activities

FY 2022 Maturity Level: 2 – Defined. OPM has defined policies and procedures for communicating planning and performance of recovery activities to stakeholders. Planning activities are communicated to management and stakeholders when contingency plans are updated. Plan performance is communicated to stakeholders in the form of an after-action report resulting from a contingency plan test or service impacting incident. OPM was able to produce some completed after action reports but stated that after action reporting has not been implemented enterprise wide. Additionally, routine testing and contingency plan maintenance is not being performed for all systems as described for Metric 62 – Contingency Plan Maintenance and Metric 63 – Contingency Plan Testing.

In the self-assessment OPM conducted, the goal maturity level for this metric was *Consistently Implemented*. We have assessed the maturity level of this metric as *Defined*. To achieve *Consistently Implemented*, the information on the planning and performance of recovery activities needs to be consistently communicated to relevant stakeholders and executive management teams. However, as we discussed in metric 63, contingency plans are not tested annually for all systems. Since metric 63 is not *Consistently Implemented*, the communication of recovery activities cannot be completed to achieve the *Consistently Implemented* maturity level. Therefore, a recommendation will not be issued for this metric.

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	1			
3 - Software Inventory	1	Level 3: Consistently Implemented	Level 2: Defined	Level 3: Consistently Implemented
4 - System Security Categorization	4			
5 - Risk Policy and Strategy	2			
6 - Information Security Architecture	1			
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	1	Supply Chain Risk Management Level 1: Ad Hoc		
13 - Implementation of SCRM	1			
14 - Ensure 3rd parties follow SCRM Requirements	1			
15 - Maintaining and Monitoring SCRM	1			
16 - SCRM Other	n/a			
17 - Configuration Mgt. Roles, Responsibilities, and Resources	2	Configuration Management Level 2: Defined	Protect Level 3: Consistently Implemented	
18 - Configuration Management Plan	2			
19 - Baseline Configurations	1			
20 - Security Configuration Settings	1			
21 - Flaw Remediation and Patch Management	2			
22 - Trusted Internet Connection Program	1			
23 - Configuration Change Control Management	3			
24 - Vulnerability Disclosure Policy	2			
25 - Configuration Management Other Information	n/a			
26 - ICAM Roles, Responsibilities, and Resources	1	Identify and Access Management Level 2: Defined		
27 - ICAM Strategy	1			
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	2			
39 - Privacy Awareness Training	1			
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 Strategy	2	Continuous Monitoring Level 2: Defined	Detect Level 2: Defined	
49 - ISCM Roles, Responsibilities, and Resources	2			
50 - Ongoing Security Assessments	2			
51 - Measuring ISCM Program Effectiveness	3			
51 - ISCM Other Information	n/a			
52 - Incident Response Policies, Procedures, Plans, and Strategies	4	Incident Response Level 4: Managed and Measurable	Respond Level 4: Managed and Measurable	
53 - Incident Roles and Responsibilities	4			
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	2	Contingency Planning Level 2: Defined	Recover Level 2: Defined	
61 - Business Impact Analysis	2			
62 - Contingency Plan Maintenance	2			
63 - Contingency Plan Testing	1			
64 - Information System Backup and Storage	1			
65 - Communication of Recovery Activities	2			
66 - Contingency Planning Other Information	n/a			

Key

Red – Level 1: Ad Hoc

Yellow – Level 2: Defined

Green – Levels 3 & 4: Consistently Implemented or higher

Appendix II – Status of Prior OIG Audit Recommendations

Rec #	Original Recommendation	Recommendation History	Current Status
1	We recommend that OPM define the procedures for maintaining its hardware inventory.	New recommendation in FY 2019	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 1
2	We recommend that OPM define policies and procedures for a centralized software inventory.	Rolled forward from FY 2018	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 2
3	We recommend that OPM define the standard data elements for an inventory of software assets and licenses with the detailed information necessary for tracking and reporting, and that it update its software inventory to include these standard data elements.	Rolled forward from FY 2017	Closed during FY 2022
4	We recommend that OPM implement system categorization levels, business impact analysis, or data driven prioritization as a method to decide the risk-based allocation of resources.	Rolled forward from FY 2021	Closed during FY 2022
5	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	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 3
6	We recommend that OPM create a cybersecurity risk register, to consistently capture and share lessons learned on the effectiveness of cybersecurity risk management processes.	Rolled forward from FY 2021	Closed during FY 2022
7	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	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 4
8	We recommend that OPM use a risk-based approach when allocating resources to effectively implement cybersecurity risk management activities with enterprise risk management processes.	Rolled forward from FY 2021	Closed during FY 2022
9	We recommend that OPM adhere to remediation dates for its POA&M weaknesses.	Rolled forward from FY 2016	Closed during FY 2022
10	We recommend that OPM update the remediation deadline in its POA&Ms when the control weakness has not been addressed by the originally scheduled deadline (i.e., the POA&M deadline should not reflect a date in the past and the original due date should be maintained to track the schedule variance).	Rolled forward from FY 2017	Closed during FY 2022
11	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.	New recommendation in FY 2019	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 6

Rec #	Original Recommendation	Recommendation History	Current Status
12	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	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 7
13	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	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 8
14	We recommend that OPM develop and implement a baseline configuration for all information systems in use by OPM.	Rolled forward from FY 2017	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 9
15	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	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 10
16	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	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 11
17	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 2022-ISAG-017 Recommendation 12
18	We recommend that the OCIO implement a process to ensure new server installations are included in the scan repository.	Rolled forward from FY 2018	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 13
19	We recommend that OPM establish an agency-wide TIC program to manage and maintain its external agency connections.	Rolled forward from FY 2021	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 14
20	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	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 15
21	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	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 16
22	We recommend that OPM define its process for provisioning, managing, and reviewing privileged accounts.	Rolled forward from FY 2021	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 17
23	We recommend that OPM routinely review remote connection event logs in accordance with its Information System Monitoring Policy.	Rolled forward from FY 2021	Closed during FY 2022
24	We recommend that OPM define the roles and responsibilities necessary for the implementation of the agency's privacy program.	Rolled forward from FY 2018	Closed during FY 2022
25	We recommend that OPM develop its privacy program by creating the necessary plans, policies, and procedures for the protection of PII.	Rolled forward from FY 2018	Closed during FY 2022

Rec #	Original Recommendation	Recommendation History	Current Status
26	We recommend that OPM implement its defined controls for FIPS-validated encryption of PII and other agency sensitive data both at rest and in transit, prevention and detection of untrusted removable media, and the destruction or reuse of media containing PII or other sensitive agency data.	Rolled forward from FY 2021	Closed during FY 2022
27	We recommend that OPM develop a process to routinely test the Data Breach Response Plan.	Rolled forward from FY 2018	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 21
28	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	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 22
29	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. Note: While OPM has performed the workforce assessment, this recommendation remains Open as the gap analysis to identify skill gaps and training needs has not been performed.	Rolled forward from FY 2021	Closed during FY 2022
30	We recommend that OPM consistently capture information to show quantitative and qualitative data for its ongoing security assessments.	Rolled forward from FY 2021	Closed during FY 2022
31	We recommend that OPM complete its development of profiling techniques on its networks and systems to more effectively detect security incidents.	Rolled forward from FY 2021	Closed during FY 2022
32	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	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 23
33	We recommend that the OCIO conduct an agency-wide BIA and incorporate the results into the system-level contingency plans. Note: While OPM has performed an agency wide BIA, this recommendation remains Open, as OPM has not incorporated the results into the system-level contingency plans.	Rolled forward from FY 2017	Closed during FY 2022
34	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	Open: Rolled forward as Report2022-ISAG-017 Recommendation 25
35	We recommend that OPM test the contingency plans for each system on an annual basis.	Rolled forward from FY 2008	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 27
36	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	Open: Rolled forward as Report 2022-ISAG-017 Recommendation 29

Appendix III

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Chief Information
Officer

Memorandum for: Eric Keehan
Chief, Information System Audit Group
Office of the Inspector General

From: Guy Cavallo
Chief Information Officer

Kellie Cosgrove Riley
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 – FY22
(Report No. 2022-ISAG-0017)

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 2022, Report No. 2022-ISAG-0017. 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 26 of the OIG's 29 recommendations and respectfully partially concurs with the remaining three recommendations.

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

Recommendation 1 (Rolled forward from 2019): We recommend that OPM define the procedures for maintaining its hardware inventory.

Management's Response: Concur. OPM has defined procedures to inventory and track all hardware assets within the Remedy Asset Management Console for a subset of the agency assets. Upon receipt of hardware, the hardware is tagged with asset tags and entered in Remedy before it is entered in inventory. Before the hardware is sent to a user, it is assigned to the user in Remedy. In FY23, OPM will expand enterprise-wide hardware asset management through a recently awarded contract to build out the inventory to include all hardware components. OPM will provide the hardware inventory documentation to OIG once we have expanded the procedures to other areas.

Recommendation 2 (Rolled forward from 2018): We recommend that OPM define policies and procedures for a centralized software inventory.

Management's Response: Concur. OPM will document policies and procedures for a centralized software inventory and will provide them to OIG upon completion.

Recommendation 3 (Rolled forward from 2017): 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.

Management's Response: Concur. After the FY22 audit fieldwork concluded, OPM completed risk assessments for the IT systems. OPM will provide evidence to support closure to OIG under separate cover.

Recommendation 4 (Rolled forward from 2017): We recommend that OPM update its enterprise architecture, to include the information security architecture elements required by NIST and OMB guidance.

Management's Response: Concur. OPM recently hired a Chief Cybersecurity Architect and an Enterprise Architect who both onboarded at the end of the FY22 fiscal year who will coordinate the integration of the enterprise security architecture into the overall enterprise architecture. A project to develop the OPM Enterprise Security Reference Model is in progress.

Recommendation 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.

Management's Response: Concur. To advance to the next FISMA maturity level of Managed and Measurable, OPM will review and update our related policies and the metric in the Information Security Continuous Monitoring Metrics document. Monitoring of this metric will be built into the current continuous monitoring dashboards in our Governance, Risk and Compliance tool and regular review will occur with our Plan of Actions and Milestones (POA&M) metrics review. We will update the POA&Ms to be manageable. After months of successful tracking, OPM will submit closure evidence to the OIG.

Recommendation 6 (Rolled forward from 2019): 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.

Management's Response: Concur. OPM is taking steps to address Supply Chain Risk Management (SCRM) requirements. The Investment Review Board (IRB) has reviewed and provided comments to the draft charter to identify the body that will be responsible for SCRM processes and activities.

Recommendation 7 (Rolled forward from 2017): 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.

Management's Response: Concur. OCIO awarded a contract that started in FY 22 to develop and document our enterprise baseline configurations for end user devices, servers, and cloud systems. OPM will submit CM evidence to the OIG under separate cover.

Recommendation 8 (Rolled forward from 2017): We recommend that OPM document the lessons learned from its configuration management activities and update its configuration management plan as appropriate.

Management's Response: Concur. OCIO awarded a contract in FY22 to develop and document our enterprise baseline configurations for end user devices, servers, and cloud systems. The configuration management program now includes those configurations. OPM will submit the evidence to the OIG under separate cover.

Recommendation 9 (Rolled forward from 2017): We recommend that OPM develop and implement a baseline configuration for all information systems in use by OPM.

Management's Response: Concur. OPM is identifying and documenting modern baseline configurations based on the current Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). We have configuration settings for recent implementations. The agency will continue documenting, testing, and implementing the exceptions and variations to the baselines.

Recommendation 10 (Rolled forward from 2014): We recommend that the OCIO develop and implement [standard security configuration settings] for all operating platforms in use by OPM.

Management's Response: Concur. Concur. OPM is identifying and documenting modern baseline configurations for the agency based on the current DISA STIGs. We patched legacy systems to update the standard security configuration settings. We will continue documenting, testing, and implementing the exceptions and variations to the baselines incorporating standard security configuration settings.

Recommendation 11 (Rolled forward from 2016): 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.

Management's Response: Concur. OPM has identified and documented all exceptions to the DISA STIGs baseline configurations for the agency end user devices. The agency will continue documenting, testing, and implementing the exceptions and variations to the baselines. OPM will submit the evidence to the OIG under separate cover.

Recommendation 12 (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's Response: Concur. As outlined in OPM's policy and procedures, POA&Ms are created for patches exceeding the mandated timeframe. Risk acceptances could be issued for patches that are managed through mitigating controls. We are updating our IT security policies and procedures to meet National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5. OPM will also review and update the patching procedures as necessary. Once finalized, OPM will provide the updated documentation to OIG.

Recommendation 13 (Rolled forward from 2018): We recommend that the OCIO implement a process to ensure new server installations are included in the scan repository.

Management's Response: Concur. OPM is adjusting processes related to our Network Access Control (NAC) and scanning tool to incorporate automation and to improve performance.

Recommendation 14 (Rolled forward from 2021): We recommend that OPM establish an agency-wide TIC program to manage and maintain its external agency connections.

Management's Response: Concur. OPM has built and implemented a Trusted Internet Connection (TIC) program over the last few years. OPM has provided OIG the capabilities and infrastructure required to participate in the TIC, Einstein and Continuous Diagnostics and Mitigation (CDM) programs. OPM has also met the Federal TIC security requirements. OPM will improve our documentation and communication of our TIC environment and will gather the required documentation for follow-up with the respective Federal authorities.

Recommendation 15 (Rolled forward from FY 2021): We recommend that OPM create a charter to govern the roles and responsibilities of its ICAM office's governance body.

Management's Response: Concur. The draft OPM Identity, Credential and Access Management (ICAM) governance charter is routing for internal concurrence. OPM will provide the documentation to OIG once it is final.

Recommendation 16 (Rolled forward from 2017): 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.

Management's Response: Concur. OPM's draft ICAM strategy is routing for internal concurrence. OPM will provide the documentation to OIG once it is final.

Recommendation 17 (Rolled forward from 2021): We recommend that OPM define its process for provisioning, managing, and reviewing privileged accounts.

Management's Response: Concur. OPM has a documented process to create, manage, and review privileged accounts. Requests for privileged accounts are submitted by a Federal Manager using a Privileged Account Request Form. Each request is reviewed and signed off by Enterprise Infrastructure Services (EIS) management. EIS Operations administrators approve and manage privileged accounts. OPM run automated reports bi-monthly to show privileged account permissions and user disablement. OPM sent the supporting documentation to OIG after the audit fieldwork concluded.

Recommendation 18: We recommend that OPM establish and document configuration and connection requirements which must be met prior to authorizing remote access.

Management's Response: Concur. OPM is implementing Zero Trust principals to address this recommendation.

Recommendation 19: We recommend that OPM acquire the identified resources for the privacy program.

Management's Response: Concur. The Office of Privacy and Information Management (OPIM) prepared a staffing plan for Fiscal Year 2023 for review by OPM's Human Resources and Strategic Hiring Committee to identify specific positions that OPIM intends to hire in FY23 to build the privacy program. OPIM will proceed with our hiring actions once the plan is approved.

Recommendation 20 (Rolled forward from 2018): 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.

Management's Response: Partially Concur. We do not concur with the recommendation insofar as it states that we do not currently have processes in place to ensure consistent performance of privacy roles and responsibilities. Within OPIM, the privacy analysts and other staff have clearly defined position descriptions, and annual performance plans that are reviewed regularly. In addition, OPIM works closely with the OCIO Cybersecurity staff and program offices to address privacy compliance requirements related to the Authorization to Operate process, to include their role in completing Privacy Threshold Analyses and Privacy Impact Assessments, as necessary. We concur with the recommendation insofar as we recognize that there are additional steps that we can take to establish more consistency across OPM and we will look for opportunities going forward, subject to other priorities and resource constraints.

Recommendation 21 (Rolled forward from 2018): We recommend that OPM develop a process to routinely test the Data Breach Response Plan.

Management's Response: Concur. The existing Breach Response Plan was issued in 2017. OPIM plans to update the plan, including developing an annual table-top exercise, as resources permit. OPIM and OCIO will also coordinate all table-top exercises.

Recommendation 22 (Rolled forward from 2018): We recommend that OPM identify individuals with heightened responsibility for PII and provide role-based training to these individuals at least annually.

Management's Response: Partially Concur. We do not concur with the recommendation to the extent it states that we have not previously identified individuals with heightened responsibility for Personal Identifiable Information (PII) and provided them with training. The OPIM has provided training in the past to supervisors, senior leadership, and other offices, such as the Office of the Chief Financial Officer, with significant responsibility for PII. We partially concur that it would be beneficial to formally document those for whom role-based training would be beneficial for the agency and to provide such training more systematically.

Recommendation 23 (Rolled forward from 2018): We recommend that OPM perform a gap analysis to determine the contingency planning requirements (people, processes, and technology) necessary to implement the agency's contingency planning policy effectively.

Management's Response: Concur. Concur. OPM will further incorporate contingency planning roles and requirements details into the appropriate training programs. We will target System Owners, Authorizing Officials, and OCIO staff. Evidence of this role clarification and training will be provided OIG.

Recommendation 24: We recommend that OPM update the BIA Worksheet template to include all criteria outlined in NIST SP 800-34, Revision 1.

Management's Response: Partially Concur. OPM consistently reviews and implements the required criteria from SP 800-34 Rev. 1. We will conduct a thorough review of the current Business Impact Analysis (BIA) Worksheet template against NIST SP 800-34, Rev. 1 during the evaluation of information systems and operations as part of contingency planning requirements and priorities planning. As a result of our review of the template against the Special Publication, OPM will document the deltas in a gap analysis. We will update the templates, as necessary and will provide the templates and gap analysis to OIG.

Recommendation 25 (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's Response: Concur. As part of current OPM Security Authorization Guide and Risk Management Framework (RMF) process, a Contingency Plan (CP) is a required element of all major systems to obtain an authorization to operate. OPM will ensure that the contingency plans are reviewed and updated as part of the plan testing process.

Recommendation 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.

Management Response: Concur. While agencies are required to follow NIST guidance in accordance with Office of Management and Budget (OMB) policy, there is flexibility within NIST's guidance in how agencies apply the guidance. Unless otherwise specified by OMB, the 800-series guidance generally allows agencies some latitude in the application. OPM has consistently reviewed and implemented the required criteria from SP 800-34 Rev 1 into the Contingency Plan development. As indicated in previous system level audits, OPM is compliant with 800-34 Rev 1 criteria.

OPM will take the required steps to ensure that the required areas of NIST SP 800-34 Rev. 1 are considered within related policies and procedures to test the contingency plans.

Recommendation 27 (Rolled forward from 2008): We recommend that OPM test the contingency plans for each system on an annual basis.

Management's Response: Concur. We are developing (when necessary) and executing POA&Ms with system owners and supported Office Heads to test the contingency plans for each system on an annual basis.

Recommendation 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.

Management Response: Concur. As OPM implements the Cloud First Strategy, we will take every opportunity to use cloud technology and FedRAMP cloud service providers. OPM is taking steps to reduce the number of cloud environments within OPM. For example, we recently transitioned our Enterprise Cost Accounting System (ECAS) to OPM's Enterprise Cloud from a third-party cloud provider. Regarding cloud backup and storage, we are evaluating and documenting available cloud data management, file system, and storage solutions. We are also evaluating and documenting the dependencies for storage scenarios and requirements. We will continually take advantage of the native cloud capabilities and features including disaster recovery and high availability. OPM will provide the documentation to OIG once it is final.

Recommendation 29 (Rolled forward from 2020): 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.

Management's Response: Concur. OPM will document security controls equivalent to the primary sites and test them through the system level assessment process, as part of the related risk management framework's phase to adequately meet the required safeguards. As we implement the Cloud First Strategy, we will take every opportunity to use cloud technology and FedRAMP cloud service providers.

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:

Anne Harkavy
Chief of Staff

Douglas Glenn
Chief Financial Officer

Mark W. 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

Marc Flaster
Senior Advisor, Office of Privacy and Information Management

Benjamin Mizer
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: https://oig.opm.gov/contact/hotline

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

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