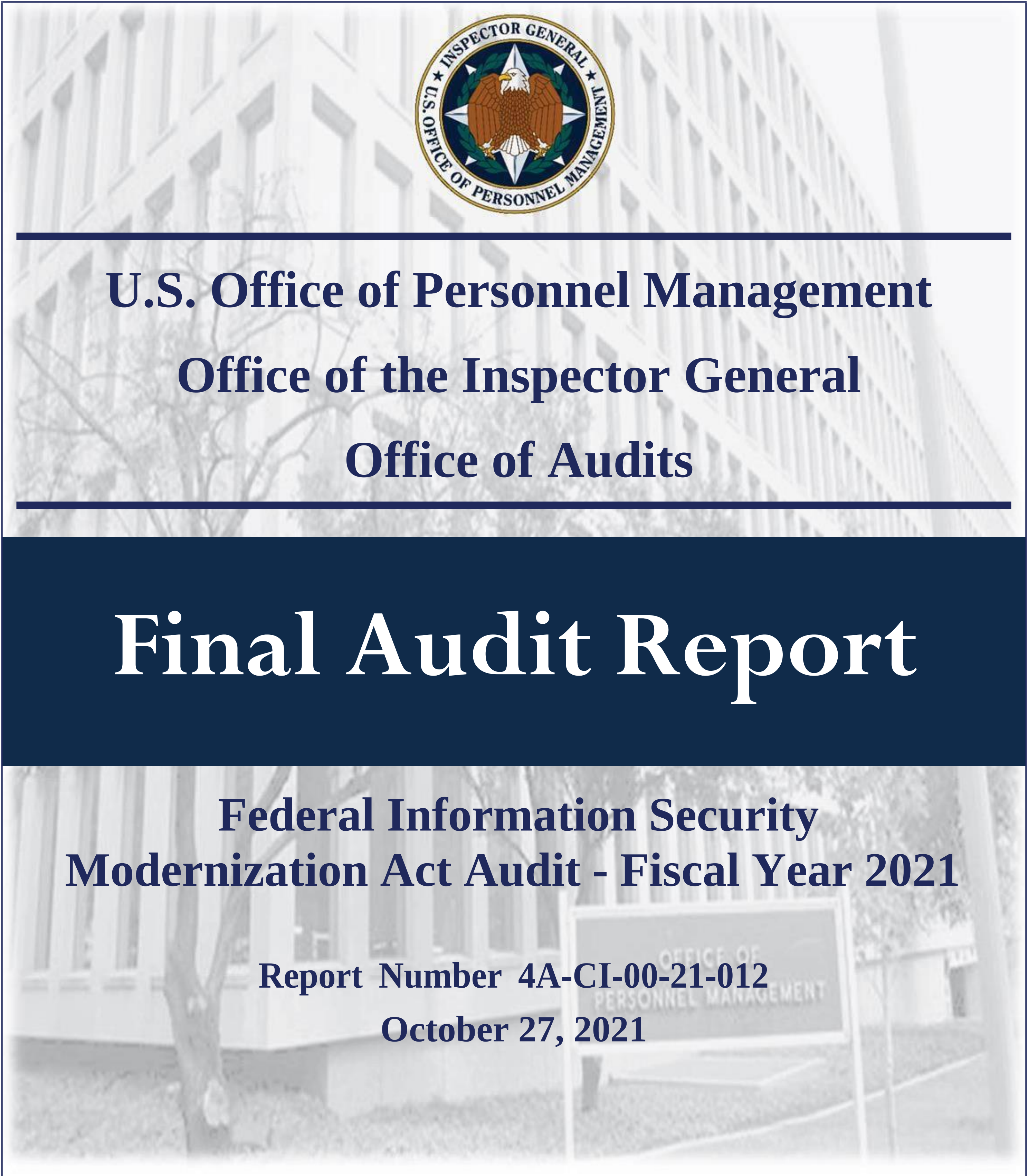


U.S. Office of Personnel Management

Office of the Inspector General

Office of Audits

Final Audit Report

Federal Information Security Modernization Act Audit - Fiscal Year 2021

Report Number 4A-CI-00-21-012

October 27, 2021

Executive Summary

Federal Information Security Modernization Act Audit - Fiscal Year 2021

Report No. 4A-CT-00-21-012 **October 27, 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 2020 through August 2021 in the Washington, D.C. area.

Michael R. Esser
Assistant Inspector General
for Audits

What Did We Find?

The Fiscal Year (FY) 2021 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 2021, OPM's cybersecurity maturity level is measured as "2 - Defined."

The following sections provide a high-level outline of OPM's performance in each of the 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 inventory.

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, OPM's privacy awareness training still needs to be developed.

Security Training - OPM has implemented a security training strategy and program. OPM has performed a workforce assessment but is still working to address gaps identified in its security training needs.

Information Security Continuous Monitoring - OPM has established many of the policies and procedures surrounding continuous monitoring, but the agency has not completed the implementation and enforcement of the policies. OPM also needs to continue to improve with conducting security controls assessments on all of 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 of the FISMA metrics at the level of Consistently Implemented or higher.

Contingency Planning - OPM has not implemented several of the FISMA requirements related to contingency planning and continues to improve upon maintaining its contingency plans as well as conducting contingency plan tests on a routine basis.

Abbreviations

Authorization	**Security Assessment and Authorization**
BIA	**Business Impact Analysis**
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

Executive Summary i

Abbreviations iii

I. **Background** 1

II. **Objective., Scope, and Methodology** 2

III. **Audit Findings and Recommendations** 5

A. Introduction and Overall Assessment 5

B. Risk Management 7

C. Supply Chain Risk Management 17

D. Configuration Management 18

E. Identity, Credential, and Access Management 25

F. Data Protection and Privacy 30

G. Security Training 35

H. Information Security Continuous Monitoring 38

I. Incident Response 41

J. Contingency Planning 44

Appendix I: Detailed FISMA Results by Metric

Appendix II: Status of Prior OIG Audit Recommendations

Appendix III: The Office of Personnel Management's October 7, 2021, response to the draft audit report, issued September 17, 2021.

Report Fraud, Waste, and Mismanagement

I. Background

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

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

FISMA reaffirms 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 Fiscal Year (FY) 2021 Inspector General FISMA Reporting Instructions. This document provides a consistent 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 FY 2021 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.

In addition, we performed audits focused on three of OPM's major information systems - the Benefits Financial Management System, the Consolidated Business Information System, and the Executive Schedule C System. We also followed-up on outstanding recommendations from prior FISMA audits.

Scope and Methodology

We conducted this performance audit in accordance with the U.S. Government Accountability Office's Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit covered OPM's FISMA compliance efforts throughout FY 2021.

We implemented a new approach this year that involved requesting 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 if we determined that OPM's maturity level was lower than its self-assessed maturity level. Additionally, 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:

- DHS Office of Cybersecurity and Communications FY 2021 Inspector General Federal Information Security Modernization Act Reporting Metrics;

- OPM Information Technology Security FISMA Procedures;

- OPM Security Assessment and Authorization Guide;

- OPM Plan of Action and Milestones Guide;

- OMB Circular A-130, Managing Information as a Strategic Resource;

- 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 Special Publication (SP) 800-12, Revision 1, An Introduction to Computer Security:
- The NIST Handbook;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information System
- NIST SP 800-53, Revision 4, 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 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations;
- NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations;
- Federal Continuity Directive 1;
- Federal Cybersecurity Workforce Assessment Act of 2015; 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 remotely from December 2020 through August 2021 in the Washington, D.C. area.

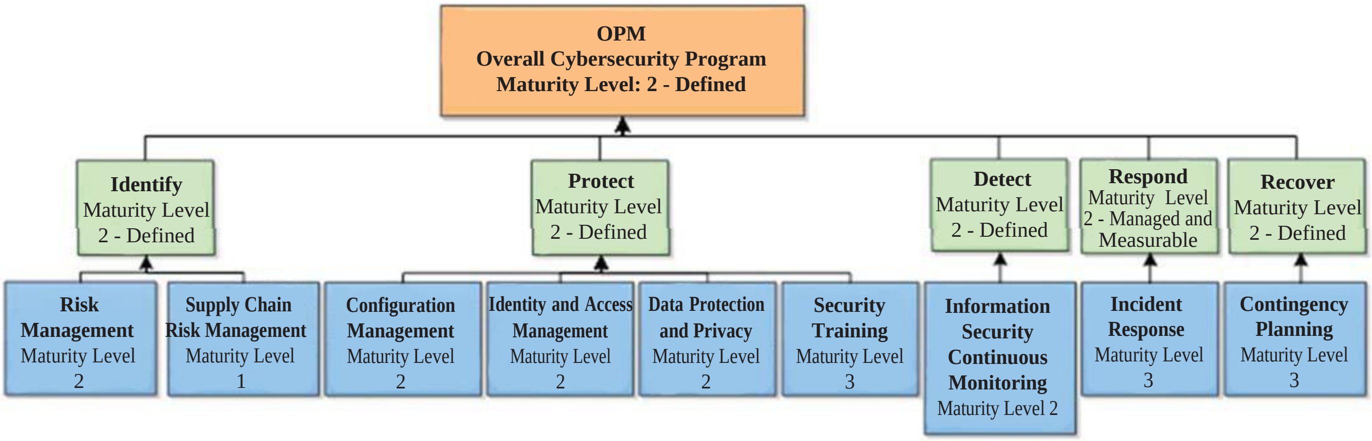
Compliance with Laws and Regulations

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 FY 2021 FISMA IG Reporting Metrics use a maturity model evaluation system derived from the NIST Cybersecurity Framework. The Cybersecurity Framework is comprised of five "function" areas that map to the nine "domains" under the function areas. This year, a new domain was added, Supply Chain Risk Management (SCRM). These nine domains are broad cybersecurity control areas used to assess the effectiveness of the information security policies, procedures, and practices of the agency. Each domain is comprised of a series of individual metrics, which are the specific controls that we evaluated and tested when assessing the agency's cybersecurity program. Each metric receives a maturity level rating of 1-5. The chart below outlines the overall maturity of OPM's cybersecurity program.



The following table outlines the description of each maturity level rating, as defined by the FY 2021 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.

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

In FY 2020, the mode (i.e., the number that appears most often) from the maturity levels of each individual metric was used to determine the corresponding domain rating and in the event of a tie between maturity levels the higher level was used. Similarly, the mode from the domain ratings determines the function area rating. In that audit report, we calculated the overall agency rating using the same methodology. This year, a new pilot concept of weighting certain metrics for scoring was introduced. 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 new SCRM domain will not be included in the calculation of the maturity rating for the Identify function.

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 "2 - *Defined*."**

Metric 1 - Inventory of Major Systems and System Interconnections

FY 2021 Maturity Level: 3 – Consistently Implemented. OPM has policies and procedures for developing an inventory of information systems. OPM policy states that Information System Security Officers (ISSO) are responsible for generating 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 authorization process. Interconnections are inventoried as a part of OPM's ISCM strategy. OPM monitors and maintains the inventories and interconnection records in its Governance, Risk, and Compliance (GRC tool.

In the self-assessment OPM conducted, this metric was assessed as *Defined* with a goal maturity level of *Managed and Measurable*. We have assessed the maturity level of this metric as *Consistently Implemented*. To achieve the *Managed and Measurable* maturity level, OPM needs to ensure that the information systems included in its inventory are subject to the monitoring processes defined within its ISCM strategy. However, as we will discuss in section H, OPM's ISCM strategy is not *Consistently Implemented*. Since the ISCM strategy is not *Consistently Implemented,* the *Managed and Measurable* maturity level cannot be achieved for this metric. Therefore, a recommendation will not be issued for this metric.

Metric 2 - Hardware Inventory

FY 2021 Maturity Level: 1 – Ad Hoc. OPM 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 utilizes tools to capture some of the information, however a central hardware repository complete with supporting procedures and processes has not been established.

In the self-assessment OPM conducted, this metric was assessed as *Ad Hoc* with a goal maturity level of *Managed and Measurable*. We have also 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 4, states that organizations with centralized inventories must "ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association [and] information system owner)."

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:

"We believe OPM is already in compliance with this recommendation. OPM has procedures to maintain the hardware inventory. We will review the procedures as necessary and will provide the documentation to OIG under separate cover."

OIG Comment:

During the audit the OCIO did not provide any evidence to support that this metric was implemented. If the OCIO believes that the recommendation is implemented, it should provide OPM's Internal Oversight and Compliance (IOC) group with evidence as part of the audit resolution process.

Metric 3 - Software Inventory

FY 2021 Maturity Level: 1 – Ad Hoc. OPM implemented a software asset management tool in FY 2021 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, this metric was assessed as *Ad Hoc* with a goal maturity level of *Managed and Measurable*. We have also 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 4, states that organizations with centralized inventories must "ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association [and] information system owner).

Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, 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. This increases the agency's susceptibility to unassessed risks and undetected vulnerabilities since agency officials are authorizing systems without a complete understanding of the included components.

Recommendation 2 (Rolled forward from 2018)

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

OPM Response:

"Concur. OPM is documenting policies and procedures for a centralized software inventory. We will provide the policies and procedures to OIG once they are complete."

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.

Recommendation 3 (Rolled forward from 2017)

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.

OPM Response:

"Concur. The Office of the Chief Information Officer (OCIO) has developed systems requirements specifications for an authoritative enterprise software registry that defines the standard data elements required to perform software management. Additionally, OCIO will continue to update the software inventory to include these standard data elements."

Metric 4 - System Security Categorization

FY 2021 Maturity Level: 3 – Consistently Implemented. OPM has policies and procedures in place to categorize its systems. ISSOs document the security categorization of their systems based on Federal Information Processing Standards Publication (FIPS) 199, NIST SP 800-60, and OPM guidance. The OPM Security Authorization Guide states that system owners, authorizing officials and the Chief Information Security Officer are involved with approving the security categorization of systems. In addition, OPM utilizes its Enterprise Business Impact Analysis to prioritize recovery of systems. However, OPM was unable to provide evidence on how risk-based allocation of resources, through collaboration and data driven prioritization, is performed.

In the self-assessment OPM conducted, this metric was assessed as *Consistently Implemented* with the goal maturity level of *Managed and Measurable*. We have also 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 4, states that, "Security categories describe the potential adverse impacts to organizational operations, organizational assets, and individuals if organizational information and information systems are compromised through a loss of confidentiality, integrity, or availability."

OMB M-19-03 states that "It is imperative that agency Chief Information Officers . , Chief Information Security Officers . , Chief Financial Officers . , Senior Agency Officials for Privacy . , or other roles, in coordination with OMB and DHS, work together to appropriately allocate agency resources for [High Value Assets] and to ensure the effective protection of [High Value Assets]."

Failure to collaborate and provide data-driven prioritization may impede visibility into high value assets that require visibility and support.

Recommendation 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.

OPM Response:

"We believe that OPM is in compliance with this recommendation. OPM instituted system categorization levels, business impact analyses, and uses risk information to prioritize the allocation of its resources. OPM is reviewing this practice and is formalizing the required evidence."

OIG Comment:

During the audit the OCIO did not provide any evidence to support that this metric was implemented. If the OCIO believes that the recommendation is implemented, it should provide IOC with the evidence as part of the audit resolution process.

Metric 5 - Risk Policy and Strategy

FY 2021 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. However, we didn't receive any evidence from OPM of a risk register or capturing and sharing lessons learned on the effectiveness of cybersecurity risk management processes and updating the program accordingly. Additionally, from a judgmental sample of 30 systems that we selected, 7 systems have not had a risk assessment performed since FY 2019, and 10 systems have not had a risk assessment performed this year. OPM's risk management policy states risk assessments should be updated annually.

In the self-assessment OPM conducted, this metric was assessed as *Ad Hoc* with a goal maturity level of *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 Risk Management Policy states, "Update the risk assessment [at least annually] or whenever there are significant changes to the information system or environment of operation . ."

Failure to consistently review and update risk assessments increases 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 5 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:

"Partially Concur. OPM has risk assessments for some systems, but not all. OPM will review the risk assessments for each major system and will take steps to ensure that control tests are included, where they are not already included. OPM will provide evidence to OIG once the review is complete."

OIG Comment:

As part of the audit resolution process, we recommend that the OCIO provide IOC with evidence once the agency has fully implemented this recommendation.

Recommendation 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.

OPM Response:

"We believe that OPM is in compliance with this recommendation. OPM created a cybersecurity risk register, periodically reviews the register, and shares lessons learned with risk owners. OPM will gather and provide evidence of the register and risk management practices to OIG under separate cover."

OIG Comment:

During the audit the OCIO did not provide any evidence to support that this metric was implemented. If the OCIO believes that the recommendation is implemented, it should provide IOC with the evidence as part of the audit resolution process.

Metric 6 - Information Security Architecture

FY 2021 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.

In the self-assessment OPM conducted, this metric was assessed as *Ad Hoc* with a goal maturity level of *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 4, 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 information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/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 7 (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 will update the enterprise architecture to include the necessary information security architecture elements. Additionally, OCIO is hiring an enterprise architect to map IT assets and to drive business strategy through information technology."

Metric 7 - Risk Management Roles, Responsibilities, and Resources

FY 2021 Maturity Level: 3 – Consistently Implemented. 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 policies addressing roles of the: Chief Information Security Officer, ISSO's, Authorizing Officials, System Owners, and the Risk Management Council. OPM provided ample evidence that the Risk Management Council meetings are occurring to provide input on metrics, policies and procedures, and status of Plans of Action and Milestones (POA&M). Evidence of performance standards were also provided by OPM, which hold Cybersecurity personnel accountable for risk management responsibilities. Currently OPM relies on their performance metrics to hold cybersecurity program managers accountable for allocating resources. In order to attain a maturity level of *Managed and Measurable*, OPM needs processes, people, and technology to be allocated by stakeholders in a risk-based manner.

In the self-assessment OPM conducted, this metric was assessed as *Consistently Implemented* with a goal maturity level of *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 800-39 describes five outcomes of governance related to organization-wide risk management which included: effective and efficient allocation of risk management resources, and performance-based outcomes by measuring, monitoring, and reporting risk management metrics to ensure that organizational goals and objectives are achieved. It also states that the risk executive (function) should coordinate with senior leaders/executives to establish risk management roles and responsibilities.

Failure to have a mature and consistent IT security program increases the risk that the information systems and environment at OPM will not meet the necessary business requirements for confidentiality, availability, and integrity.

Recommendation 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.

OPM Response:

"We believe that OPM is in compliance with this recommendation. OPM uses a risk-based approach when allocating resources for cybersecurity risk management activities."

OIG Comment:

During the audit the OCIO did not provide any evidence to support that this metric was implemented. If the OCIO believes that the recommendation is implemented, it should provide IOC with the evidence as part of the audit resolution process.

Metric 8 - Plan of Action and Milestones

FY 2021 Maturity Level: 2 – Defined. OPM has thoroughly defined and communicated policies and procedures for the effective use of POA&Ms. 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 uses the GRC tool as a risk repository and a means to track the status of POA&Ms to effectively mitigate security weaknesses in a timely manner. OPM's ISCM metrics have a target of 95% of POA&M deadlines being current. We analyzed all 887 open POA&Ms located in the GRC tool. Our analysis identified that over 60% of the POA&Ms were overdue. More specifically, as of August 23, 2021, we noted the following:

- 34% of POA&Ms were over 12 months overdue;
- 11% of POA&Ms were 7 - 12 months overdue ;
- 2% of POA&Ms were 4-6 months overdue; and
- 15% of POA&Ms were 1-3 months overdue.

In the self-assessment OPM conducted, this metric was assessed as *Consistently Implemented* with a goal maturity level of *Managed and Measured*. 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 recommendations are to assist OPM with attaining the *Consistently Implemented* maturity level.

NIST SP 800-53 Revision 4 states that "The organization . Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system . ." It also states, "Updates existing plan of action and milestones [organization-defined frequency] based on the findings from controls assessments, independent audits or reviews, and continuous monitoring activities."

Tracking, updating, remediating, and closing POA&Ms are vital to diagnosing a system's level of risk, which impacts how that system affects the overall risk to OPM. Without up-to-date POA&Ms OPM is unable to make effective risk-based decisions and distribute resources efficiently to address risk.

Recommendation 9 (Rolled forward from 2016)

We recommend that OPM adhere to remediation dates for its POA&M weaknesses.

OPM Response:

"Partially Concur. OPM has instituted metrics and processes to identify, monitor, and track the completion of Plan of Action & Milestones (POA&Ms). We will re-baseline when slippage occurs."

OIG Comment:

We agree that OPM has instituted metrics and processes to identify, monitor and track the completion of POA&Ms. However, as we stated above, our analysis identified that over 60% of open POA&Ms were overdue. OPM is not meeting its target of 95% of POA&M deadlines being current. Action still needs to be taken to ensure POA&Ms adhere to remediation dates.

The end of OPM's response to the OIG recommendations included Technical Comments related to the POA&M testing results stated above. The Technical Comments state that our POA&M testing inappropriately included systems that belong to the Defense Counterintelligence and Security Agency. However, those systems were included because at the time of testing, the POA&Ms for those systems were open and OPM ISSOs were assigned to the POA&Ms. Additionally, even with the exclusion of the Defense Counterintelligence and Security Agency systems, the Technical Comments state that the total number of overdue POA&Ms is still 13% of all open POA&Ms. Therefore, our finding and recommendation for metric 8 are still valid.

Recommendation 10 (Rolled forward from 2017)

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).

OPM Response:

"Partially Concur. OPM has instituted metrics and processes to identify, monitor, and track the completion of Plan of Action & Milestones (POA&Ms). We will re-baseline when slippage occurs."

OIG Comment:

We agree that OPM has instituted metrics and process to identify, monitor and track the completion of POA&Ms. However, as we stated above, our analysis identified that over 60% of open POA&Ms are overdue. OPM is not meeting its target of 95% POA&M deadlines being current. Action still needs to be taken to ensure that POA&M remediation deadlines are updated when the control weakness has not been addressed by the originally scheduled deadline.

Metric 9 - Risk Communication

FY 2021 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 regards to 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, this metric was assessed as *Consistently Implemented* with a goal maturity level of *Consistently Implemented*. We have also assessed this metric as *Consistently Implemented*.

Metric 10 - Centralized Enterprise-wide Risk Tool

FY 2021 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 risk/weakness 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 system inventory 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 management dashboard.

In the self-assessment OPM conducted, this metric was assessed as *Ad Hoc* with a goal maturity level of *Defined*. 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 2021 Maturity Level: 1 – Ad Hoc. The SCRM domain is new for FY 2021 and the final metrics were not issued until the middle of audit fieldwork. OPM did not provide a self - assessment of this domain. Further, OPM did not provide any evidence for the metric to demonstrate achievement of a maturity level. Therefore, the default maturity level for the metric is *Ad Hoc*. 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 11 (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 will take the steps necessary to address supply chain risk management requirements."

Metric 13- SCRM Policies and Procedures

FY 2021 Maturity Level: 1 – Ad Hoc. OPM did not provide a self -assessment of this domain. Further, OPM did not provide any evidence for this metric to demonstrate achievement of a maturity level. 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 2021 Maturity Level: 1 – Ad Hoc. OPM did not provide a self -assessment of this domain. Further, OPM did not provide any evidence for this metric to demonstrate achievement of a maturity level. 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 2021 Maturity Level: 1 – Ad Hoc. OPM did not provide a self -assessment of this domain. Further, OPM did not provide any evidence for this metric to demonstrate achievement of a maturity level. 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 2021 Maturity Level: 2 – Defined. OPM has policies and procedures in place defining CM stakeholders and their roles and responsibilities. However, an appropriate gap analysis has not been performed in order for OPM to adequately address that 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, this metric was assessed as *Defined* with a goal maturity level of *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."

Without adequate resources to manage CM operations, there is an increased risk of improperly configured devices on the network and an increased threat of malicious attacks.

Recommendation 12 (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. OPM recently awarded a technology contract to develop enterprise configuration management standards and the automated processes to implement and maintain the standards.”

Metric 18 - Configuration Management Plan

FY 2021 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 its change control process.

In the self-assessment OPM conducted, this metric was assessed as *Defined* with a goal maturity level of *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 13 (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. OPM recently awarded a technology contract to develop enterprise configuration management standards and the automated processes to implement and maintain the standards."

Metric 19 - Baseline Configurations

FY 2021 Maturity Level: 1 – Ad Hoc. OPM has not developed a baseline configuration for all of its information systems.

NIST SP 800-53, Revision 4, 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."

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

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, this metric was assessed as *Ad Hoc* with a goal maturity level of *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 4, advises that an "organization develops, documents, and maintains under configuration control, a current baseline configuration of the information 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 14 (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 has configuration settings for recent implementations. The configuration settings will be presented to OIG under separate cover. We are developing and implementing standard configuration settings for legacy and older OPM information systems. We will continually implement the standard configuration settings for new deployments of operating platforms through enhancements to the Enterprise Configuration Management process."

Metric 20 - Security Configuration Settings

FY 2021 Maturity Level: 1 – Ad Hoc. OPM uses the Defense Information Systems Agency's Security Technical Implementation Guides as the basis for its configuration settings. However, OPM has not consistently implemented the process for documenting and approving exceptions, which means OPM has not customized the configuration settings for its systems and environment. As a result, testing against the Defense Information Systems Agency's Security Technical Implementation Guides is not effective since OPM has not documented the allowed deviations.

In the self-assessment OPM conducted, this metric was assessed as *Ad Hoc* with a goal maturity level of *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 4, defines configuration settings as "the set of parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system." It also states, "Security-related parameters are those parameters impacting the security state of information systems including the parameters required to satisfy other security control requirements. Security-related parameters include, for example: (i) registry settings; (ii) account, file, directory permission settings; and (iii) settings for functions, ports, protocols, services, and remote connections."

NIST SP 800-53, Revision 4, requires that the organization "Establishes and documents configuration settings for information technology products employed within the information system . . . that reflect the most restrictive mode consistent with operational requirements . ."

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

Recommendation 15 (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. The CIO has determined that the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) will be the primary baseline for all OPM configuration settings of information systems. The DISA STIG will be modified to meet OPM's non-military requirements. Those modifications will be documented and provided to OIG under separate cover. We patched older/legacy systems to ensure standard security configuration settings are consistently updated."

Recommendation 16 (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 is using standard security configuration settings based on DISA's STIG for all operating platforms. We will request approval for deviations and document deviations from the standard security configuration settings in the system configuration baseline."

Metric 21 - Flaw Remediation and Patch Management

FY 2021 Maturity Level: 2 – Defined. OPM routinely performs automated vulnerability and patch compliance scans on its systems. While OPM's vulnerability scanning program has been updated over the last year, our audit test work indicated that several problems still exist. Specifically, we analyzed historical vulnerability scan results conducted by OPM for approximately 300 servers from January 2021 through April 2021 from OPM's server inventory. After reviewing the results, we identified approximately 30 critical or high findings that were past their 30-day remediation deadline.

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, this metric was assessed as *Defined* with a goal maturity level of *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 4, advises that an organization "Scans for vulnerabilities in the information system and hosted applications" and that the organization "Identifies, reports, corrects information system flaws" and "Installs security-relevant software and firmware 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 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.

OPM Response:

"Partially Concur. OPM is in compliance for end-user devices and servers. We will review the target timeframe to apply patches to the mainframes to confirm that we are conforming to a 30 day window."

OIG Comment:

Our testing identified critical or high findings that were past their 30-day remediation deadline in approximately 300 servers from January 2021 through April 2021. If OPM has since implemented the recommendation, then as part of the audit resolution process, we recommend that the OCIO provide IOC with evidence that the agency implemented this recommendation.

Recommendation 18 (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:

"Partially Concur. The new practice [is] that servers [will] be included in the scan repository. We will document the new practice and provide evidence to OIG."

OIG Comment:

If OPM has implemented the recommendation, then as part of the audit resolution process, we recommend that the OCIO provide IOC with evidence that the agency implemented this recommendation.

Metric 22 - Trusted Internet Connection Program

FY 2021 Maturity Level: 1 – Ad Hoc. In FY 2020, OPM had defined and implemented controls to monitor and manage its approved trusted internet connections (TIC). However, in FY 2021, OPM did not provide any evidence to demonstrate that the controls for this metric improved or are still in place.

In the self-assessment OPM conducted, this metric was assessed as *Consistently Implemented* with a goal maturity level of *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 government-wide cybersecurity incident response or other cybersecurity matters."

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

Recommendation 19

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

OPM Response:

"Non-Concur. OPM TIC is currently located in the Boyers data center."

OIG Comment:

In FY 2020, OPM provided evidence that the TIC program was defined and implemented. However, this year, we did not receive any evidence to indicate that the controls are still in place. If OPM has implemented the recommendation, then as part of the audit resolution process, we recommend that the OCIO provide IOC with evidence that the agency implemented this recommendation.

Metric 23 - Configuration Change Control Management

FY 2021 Maturity Level: 3 – Consistently Implemented. OPM has developed and documented policies and procedures for controlling configuration changes. The policies address the necessary change control steps and documentation required to approve information system changes.

Our test work indicated that OPM has updated its configuration change control process to include project plans and additional reviews and approvals and is consistently adhering to its change control procedures.

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

Metric 24 - Vulnerability Disclosure Policy

FY 2021 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 after OPM conducted its self-assessment, so current maturity levels were provided. 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, and for the right reason. While OPM has room for maturity in this area, the agency has successfully defined many Identity, Credential, and Access Management (ICAM) related security controls. 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

FY 2021 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 has not developed a comprehensive ICAM strategy and has not developed a plan to meet the requirement.

OPM has not developed a comprehensive ICAM strategy.

In the self-assessment OPM conducted, this metric was assessed as *Defined* with a goal maturity level of *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 OPMs ability to coordinate the ICAM program and provide effective oversight.

Recommendation 20

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

OPM Response:

"Concur. OPM is taking an enterprise approach to Identity, Credential, and Access Management (ICAM). The Chief Technology Officer (CTO) came onboard in late FY 2021 and will lead the ICAM strategy. OPM will aim to create a charter to govern the roles and responsibilities of the ICAM governance body."

Metric 27 - ICAM Strategy

FY 2021 Maturity Level: 1 – Ad Hoc. OPM has not developed 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 program, as appropriate. Milestones for meeting the requirements of Federal Initiatives should be incorporated in a comprehensive ICAM policy, strategy, process, and technology solution road map. However, OPM has not developed these or a plan to meet the requirement.

In the self-assessment OPM conducted, this metric was assessed as *Ad Hoc* with a goal maturity level of *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 [Continuous Diagnostics and Mitigation (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 achieve the Federal ICAM initiatives.

Recommendation 21 (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. The CIO has applied an enterprise view to ICAM. The CTO recently came on board and is responsible for the ICAM strategy. The CTO will coordinate with the CISO and EIS to review current ICAM practices, identify gaps, and develop action plans and milestones. We aim to complete the analysis in Q2 of FY 2022. We will provide the analysis and milestones to OIG once they are complete."

Metric 28 - Personnel Risk

FY 2021 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented processes for assigning personnel risk designations and performing appropriate screenings prior to granting access to its systems. Additionally, OPM re-screens individuals when they change positions, or the risk designation of their current position is changed.

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

Metric 29 - Access Agreements

FY 2021 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented centralized processes for developing, documenting, and maintaining access agreements for all users of the network. All personnel are required to review and acknowledge access agreements upon hire and on an annual basis thereafter, as a part of IT Security and Privacy Awareness training.

In FY 2021, OPM changed its policy to grant new personnel network access first and allow up to five days to review and sign access agreements before access is revoked.

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

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

FY 2021 Maturity Level: 3 – Consistently Implemented. OPM enforces multi-factor authentication for non-privileged users of its facilities, systems, and networks using PIV cards. Digital identity risk assessments are performed for each system to ensure that authentication processes provide the appropriate level of assurance.

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

Metric 31 - Strong Authentication Mechanisms for Privileged Users

FY 2021 Maturity Level: 3 – Consistently Implemented. OPM enforces multi-factor authentication for privileged users of its facilities, systems, and networks using PIV cards. OPM utilizes tools including an enterprise password vault to manage privileged user access to the OPM network and its back-end servers. Digital identity risk assessments are performed for each system to ensure that authentication processes provide the appropriate level of assurance.

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

Metric 32 - Management of Privileged User Accounts

FY 2021 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 and tracking, inventorying, validating, and logging and reviewing privileged users' accounts.

In the self-assessment OPM conducted, this metric was assessed as *Consistently Implemented* with a goal maturity level of *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 4, states that the organization develops and documents "Procedures to facilitate the implementation of the access control policy and associated access controls . ."

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

Recommendation 22

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

OPM Response:

"We believe that OPM is in compliance with this recommendation. We are provisioning, managing, and reviewing privileged accounts in compliance with the Continuous Diagnostics and Mitigation (CDM) requirement."

OIG Comment:

During the audit the OCIO did not provide any evidence to support that this metric was implemented. If the OCIO believes that the recommendation is implemented, it should provide IOC with the evidence as part of the audit resolution process.

Metric 33 - Remote Access Connections

FY 2021 Maturity Level: 2 – Defined. 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 remote connection event logs are reviewed based on risk.

In the self-assessment OPM conducted, this metric was assessed as *Managed and Measurable* with a goal maturity level of *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 800-53, Revision 4, states that the organization monitors the information system to detect unauthorized remote connections and identifies unauthorized use of the information system.

OPM's Information System Monitoring Policy states, "Review and analyze information system audit records [daily through automated methods or weekly though manual methods] for indications of [unauthorized use of the system]."

Failure to review audit records for unauthorized remote connections and unauthorized use of the information system increases the risk that malicious activity will be undetected.

Recommendation 23

We recommend that OPM routinely review remote connection event logs in accordance with its Information System Monitoring Policy.

OPM Response:

"Non-Concur. OPM is in compliance with this recommendation and routinely review our remote connection event logs."

OIG Comment:

In FY 2020, OPM provided evidence that remote connection event logs were routinely reviewed. However, this year, we did not receive evidence that the process is still occurring. If OPM has implemented the recommendation, then as part of the audit resolution process, we recommend that the OCIO provide IOC with evidence that the agency implemented 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 "2 - *Defined*."**

Metric 35 - Data Protection and Privacy Policies and Procedures

FY 2021 Maturity Level: 1 – Ad Hoc. The OPM Information Security and Privacy Policy Handbook is OPM's primary source for data protection and privacy policies. However, this handbook has not been updated since 2011 and does not contain the personally identifiable information (PII) protection plans, policies, and procedures necessary for a mature privacy program. The Chief Privacy Officer position was established in 2016. Additionally, roles and responsibilities for the effective implementation of OPM's privacy program have not been defined.

In the self-assessment OPM conducted, this metric was assessed as *Ad Hoc* with a goal maturity level of *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 800-53, Revision 4, requires that an organization "Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures . ."

Without a mature privacy program in place, OPM is at an increased risk of data loss and mishandling of sensitive information.

Recommendation 24 (Rolled forward from 2018)

We recommend that OPM define the roles and responsibilities necessary for the implementation of the agency's privacy program.

OPM Response:

"Partially Concur. The Office of Privacy and Information Management (OPIM) and its roles and responsibilities were approved and established by the former Acting Director as a stand-alone office in February 2019. Artifacts have been provided to the OIG over the succeeding years to document OPIMs functions and duties. As resources permit, we will continue to develop and reinforce these roles and responsibilities at the Agency."

OIG Comment:

This recommendation has been rolled forward since 2018 as we have not received evidence in prior years of defined roles and responsibilities for the privacy program. During the course of this audit, we again did not receive evidence of defined roles and responsibilities for the privacy program. Additionally, we were informed that the Office of Privacy and Information Management (OPIM) would be undergoing organizational changes. In a response, OPIM stated that "As announced by the Acting Director on May 27, 2021, the OPIM will merge with the Executive Secretariat organization shortly, and there may be subsequent changes in roles and responsibilities once the new organization takes shape. We will provide you with the appropriate documents once the reorganization and position structure are finalized." 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.

Recommendation 25 (rolled forward from 2018)

We recommend that OPM develop its privacy program by creating the necessary plans, policies, and procedures for the protection of PII.

OPM Response:

"Partially Concur. OPIM has established and communicated our policies, templates, and guidance regarding the privacy program plan through a wide range of tools including positioning documents and information on THEO for our employees. We have established a public-facing OPM web page devoted to privacy including our published Systems of Records

Notices, Privacy Impact Assessments, and Computer Matching Agreements. The web pages are updated regularly as new documents are prepared. We continue to guide program offices and the CIO offices on Privacy Threshold Analysis (PTA) and Privacy Impact Assessments (PIA) compliance documents. We collaborated with the CIO in preparing the privacy awareness module on protecting Personally Identifiable PII for the 2021 IT Security and Privacy Awareness mandated training. We will be updating the previously published OPM Security and Privacy Policy Handbook or reasonable alternatives to reflect the current state of privacy policy."

OIG Comment:

During the course of the audit, we did not receive the aforementioned policies, templates and guidance. Additionally, the OPM Security and Privacy Policy Handbook we reviewed was last updated in 2011. 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 36 - Data Protection and Privacy Controls

FY 2021 Maturity Level: 2 – Defined. OPM has defined and communicated its controls to protect sensitive information in its environment. The controls include the use of FIPS-validated encryption of PII and other agency sensitive data both at rest and in transit, controls to prevent and detect untrusted removable media, and controls related to the destruction or reuse of media containing PII or other sensitive agency data. However, OPM did not provide any evidence that these controls are implemented.

In the self-assessment OPM conducted, this metric was assessed as *Consistently Implemented* with a goal maturity level of *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 4, states that the organization "Develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technology involving PII . ."

Failure to implement defined data protection and privacy controls may compromise the confidentiality of sensitive data.

Recommendation 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.

OPM Response:

"Partially Concur. OPM has defined and communicated its controls to protect sensitive information in its environment. The controls include the use of FIPS validated encryption of PII and other agency sensitive data both at rest and in transit, controls to prevent and detect untrusted removable media, and controls related to the destruction or reuse of media containing PII or other sensitive agency data."

OIG Comment:

We agree that OPM has defined and communicated its controls to protect sensitive information in its environment. However, we did not receive any evidence that the controls were implemented. If OPM has implemented the recommendation, then as part of the audit resolution process, we recommend that the OPIM provide OPM's IOC with evidence that the agency implemented this recommendation.

Metric 37 - Data Exfiltration Prevention

FY 2021 Maturity Level: 4 – Managed and Measurable. OPM has defined policies to prevent data exfiltration from its IT environment and to implement enhanced network defenses. OPM has implemented controls to monitor inbound and outbound network traffic, as well as ensure that all traffic passes through a web content filter. In addition, OPM has implemented a process to measure the effectiveness of the controls on an ongoing basis.

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

Metric 38 - Data Breach Response Plan

FY 2021 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, this year, OPM has not updated or tested its Data Breach Response Plan.

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

In the self-assessment OPM conducted, this metric was assessed as *Defined* with the goal maturity level of *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 800-122, 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 test the Data Breach Response Plan routinely 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 27 (Rolled forward from 2018)

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

OPM Response:

"Concur. The existing Data Breach Response Plan was issued in 2017. OPIM will update the Data Breach Response Plan and develop and implement an annual table-top exercise to test the plan as resources permit during the next fiscal year."

Metric 39 - Privacy Awareness Training

FY 2021 Maturity Level: 1 – Ad Hoc. OPM has not defined its privacy awareness training program based on the organizational requirements, culture, and the types of PII that its users have access to. In addition, the organization has not developed role-based privacy training for individuals having responsibility for PII or activities involving PII.

In the self-assessment OPM conducted, this metric was assessed as *Ad Hoc* with the goal maturity level of *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, "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 28 (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. OPIM has conducted role-based training for supervisors on privacy via the bi-weekly supervisory meetings held by HR. We will work to catalog additional role-based training across other positions and aim to provide role-based training to individuals in those positions as time and resources permit."

OIG Comment:

During the course of the audit, we did not receive evidence of role-based training for privacy. 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 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 2021 Maturity Level: 3 – Consistently Implemented. OPM has established an agency-wide IT security awareness training program. Roles and responsibilities for stakeholders are defined and communicated across the agency. OPM continues to mature its security training program by consistently collecting and analyzing performance measures of the training activities.

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

Metric 42 - Assessment of Workforce

FY 2021 Maturity Level: 2 – Defined. OPM assessed the knowledge, skills, and abilities of its workforce as the first step to determine employees' specialized training needs. While OPM completed a workforce assessment in 2018, it is our understanding that there has been turnover in the workforce since the last assessment was completed. Although OPM has made progress in this area, a current gap analysis to determine any weaknesses and specialized training needs must be performed to achieve the *Consistently Implemented* maturity level.

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

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

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

Recommendation 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.

OPM Response:

"We believe that OPM is in compliance with this recommendation. We have performed the workforce assessment. We have also performed the gap analysis to identify the skills gaps and training needs."

OIG Comment:

During the audit the OCIO did not provide any evidence to support that this metric was implemented. If the OCIO believes that the recommendation is implemented, it should provide IOC with the evidence as part of the audit resolution process.

Metric 43 - Security Awareness Strategy

FY 2021 Maturity Level: 2 – Defined. In FY 2021, the security awareness and training strategy has been fully developed to maintain a security awareness program tailored to the mission and risk environment.

In the self-assessment OPM conducted, this metric was assessed as *Defined* with a goal maturity level of *Consistently Implemented*. We have assessed the maturity level of this metric as *Defined*. OPM has not consistently implemented its agency-wide security awareness and training strategy as there has been only one gap analysis performed since 2018. As stated in metric 42, a periodic re-assessment should be performed. Therefore, a recommendation will not be issued for this metric.

Metric 44 - Tracking IT Security Training

FY 2021 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 of OPM's employees and contractors completed the security awareness training course in FY 2021.

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 45 - Tracking Specialized IT Security Training

FY 2021 Maturity Level: 4 – Managed and Measurable. OPM employees with significant information security responsibilities are required to take specialized security training in addition to the annual awareness training. The OCIO uses a database to track the security training taken by employees identified as having security responsibility. One example of the specialized training program involves the OCIO conducting targeted phishing exercises/emails for individuals with security responsibilities, tracking the exercise results, and following up as needed.

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

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 2021 Maturity Level: 2 – Defined. OPM has developed ISCM strategies that address 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 established 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, this metric was assessed as *Defined* with the goal maturity level of *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 2021 Maturity Level: 2 – Defined. OPM has defined the structure, roles, and responsibilities of its ISCM teams and stakeholders. OPM conducted an analysis that identified and quantified resource gaps in the ISCM program during FY 2019. OPM has made progress filling those gaps over the past two fiscal years.

In the self-assessment OPM conducted, this metric was assessed as *Defined* with the goal maturity level of *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 2021 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 2021 for all 46 of OPM's major systems. Of those, only 40 systems were subject to security controls testing that complied with OPM's requirements for both quarters. Although OPM's cybersecurity program has addressed the resource limitations, OPM is not conducting quarterly testing on all systems.

2) System Authorizations

Of the 46 system Authorizations we reviewed, 8 were signed by agency officials no longer with OPM, a situation that necessitates re-authorization by the new Authorizing Official. Another three systems have expired Authorizations.

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

Metric 50 - Measuring ISCM Program Effectiveness

FY 2021 Maturity Level: 2 – Defined. 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. However, we did not observe any qualitative and quantitative performance measures captured for the 40 systems that completed the ongoing security controls assessments.

In the self-assessment OPM conducted, this metric was assessed as *Defined* with the goal maturity level of *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 800-137 states that an organization must "Analyze the data collected and Report findings, determining the appropriate response."

Failure to consistently capture the performance measures can impede OPM's ability to evaluate the effectiveness of the ISCM program.

Recommendation 30

We recommend that OPM consistently capture information to show quantitative and qualitative data for its ongoing security assessments.

OPM Response:

"We believe that OPM is in compliance with this recommendation."

OIG Comment:

During the audit, the OCIO did not provide any evidence to support that this metric was implemented. If the OCIO believes that the recommendation is implemented, it should provide IOC with the evidence as part of the audit resolution process.

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 consistently implemented 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 2021 Maturity Level: 4 – Managed and Measurable. OPM's incident response policies, procedures, plans, and strategies have been defined, communicated, and consistently implemented. OPM monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response program and is consistently capturing and sharing lessons learned to implement updates to the program as appropriate.

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

Metric 53 - Incident Roles and Responsibilities

FY 2021 Maturity Level: 4 – Managed and Measurable. OPM has defined roles and responsibilities related to incident response, and its incident response teams have adequate resources (people, processes, and technology) to manage and measure the effectiveness of incident response activities.

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

Metric 54 - Incident Detection and Analysis

FY 2021 Maturity Level: 3 – Consistently Implemented. OPM utilizes a classification system for its incident response program, allowing the agency to quickly analyze and prioritize any reported or detected incidents. In addition, OPM has implemented several security tools to analyze activity patterns to identify precursors and indicators of security threats to prevent security incidents.

In the self-assessment OPM conducted, this metric was assessed as *Consistently Implemented* with the goal maturity level of *Managed and Measurable*. We have assessed this metric as *Consistently Implemented*. To achieve Managed and Measurable, OPM needs to utilize profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can more effectively detect security incidents.

OPM is in the process of developing profiling techniques on its networks and systems so that it can more effectively detect security incidents. The following recommendation is to assist OPM with attaining the *Managed and Measurable* maturity level.

NIST SP 800-53, Revision 4, states that an organization "Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery _ ."

The utilization of profiling techniques to measure the characteristics of expected activities on its networks and systems increases the likelihood that security incidents will be detected more effectively.

Recommendation 31

We recommend that OPM complete its development of profiling techniques on its networks and systems to more effectively detect security incidents.

OPM Response:

"Partially Concur. We have implemented profiling techniques for some enterprise systems. We continue to expand the techniques to other systems."

OIG Comment:

It was our understanding that OPM was still in the process of developing profiling techniques. If OPM has implemented profiling techniques for the majority of systems in its inventory, then as part of the audit resolution process, we recommend that OPM provide IOC with evidence that the agency implemented this recommendation.

Metric 55 - Incident Handling

FY 2021 Maturity Level: 4 – Managed and Measurable. OPM has defined its processes for incident handling in an incident response manual. The processes include containment strategies for various types of major incidents, eradication activities to eliminate components of an incident, and mitigation techniques for exploited vulnerabilities. OPM uses metrics to measure the impact of successful incidents and is quickly able to mitigate related vulnerabilities on other systems so that they are not subject to the same exploitation.

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

Metric 56 - Sharing Incident Response Information

FY 2021 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, 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 57 - Contractual Relationships in Support of Incident Response

FY 2021 Maturity Level: 4 – Managed and Measurable. OPM collaborates with DHS and other parties, when needed, for technical assistance, surge resources, and any special requirements for quickly responding to incidents. OPM uses third party contractors, when needed, to support incident response processes. OPM also utilizes software tools provided by DHS for intrusion detection and prevention capabilities.

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

Metric 58 - Technology to Support Incident Response

FY 2021 Maturity Level: 4 – Managed and Measurable. OPM identified and fully defined its requirements for the 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 for monitoring and analyzing qualitative and quantitative incident response performance across the agency. OPM uses the data collected from these tools to generate monthly reports for stakeholders on the effectiveness of its incident response program.

In the self-assessment OPM conducted, this metric was assessed as *Managed and Measurable* with the goal maturity level of *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 2021 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.

OPM recently appointed a Senior Advisor to the CIO to lead and manage the contingency planning effort. At his appointment, he sent an email to members of OPM's Emergency Relocation Group to inform them of their continuity of operations responsibilities. While OPM is making progress, we continue to see a lapse in contingency plan maintenance and testing leading to updates performed in an ad hoc manner.

In the self-assessment OPM conducted, this metric was assessed as *Defined* with the goal maturity level of *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 32 (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 is performing a gap analysis and updating the contingency plans to modify the requirements."

Metric 61 - Business Impact Analysis

FY 2021 Maturity Level: 2 – Defined. Identifying an organization's essential mission and the risks facing its business functions is a critical element in developing contingency plans. OPM currently has a process in place to develop a Business Impact Analysis (BIA) at the information system level.

In addition, OPM successfully performed an agency-wide BIA in April 2020 as a part of the National Continuity Program. While Contingency of Operations Planning artifacts are in the process of being updated, OPM will not complete the update of the BIA until FY 2022.

Additionally, OPM has not incorporated the results of this BIA into the system-level contingency plans. Currently, it is the responsibility of the system owners and authorizing officials to ensure that BIA results are communicated and reflected in system-level contingency plans.

In the self-assessment OPM conducted, this metric was assessed as *Defined* with a goal maturity level of *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 4, advises that the agency develop "a contingency plan for information systems that . Identifies essential missions and business functions and associated contingency requirements - ."

Federal Continuity Directive 1 requires agencies to complete "a Business Impact Analysis . . . for all threats and hazards, and all capabilities associated with the continuance of essential functions at least every two years."

Outdated or inaccurate BIAs increase the risk that the agency would be unable to prioritize recovery operations effectively in the event of a service-impacting incident.

Recommendation 33 (Rolled forward from FY 2017)

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.

OPM Response:

"Concur. OPM will reflect the agency-wide Business Impact Analysis (BIA) results in the system-level contingency plans that we are updating."

Metric 62 - Contingency Plan Maintenance

FY 2021 Maturity Level: 2 – Defined. OPM has developed policies and procedures for contingency planning. OPM is also in the process of supplementing existing policies and procedures with additional materials as developed or refined by the newly appointed OCIO Contingency of Operations Planning Manager. However, OPM has not updated system-level contingency plans annually.

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

Outdated or inaccurate 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 34 (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. OCIO has contingency plans for systems that were implemented recently. We will provide those plans under separate cover. We will review the contingency plans for older/legacy systems to verify that they are up to date. We will conduct gap analysis and annual reviews for recent and older/legacy systems."

Metric 63 - Contingency Plan Testing

FY 2021 Maturity Level: 2 – Defined. Routinely testing contingency plans 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 IT contingency test plan and oversees the IT contingency plan testing process. Like last year, OPM has not effectively performed annual contingency plan testing for all systems within its inventory.

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

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

OPM policy requires system owners to "Test the contingency plan for the information system [at least annually] - ."

Failure to perform contingency plan testing for every major information system increases the risk that the agency will be unable to restore operations effectively and efficiently in the event of a service-impacting incident.

Recommendation 35 (Rolled forward from 2008)

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

OPM Response:

"Concur. The OCIO will conduct a gap analysis. Once the gap analysis is complete, OPM will test the contingency plans for each system on an annual basis with each system's Program Management Office including the system owners and authorizing officials."

Metric 64 - Information System Backup and Storage

FY 2021 Maturity Level: 2 - Defined. OPM policy defines controls for data backup, recovery and testing. OPM has also established information system backup procedures for designated staff to complete to support the contingency planning efforts. System-level contingency plan templates include a section for data backup with procedures for ensuring a timely full-system restoration. It also includes sections for alternate processing procedures and alternate storage site information.

However, we did not observe any evidence that OPM performs controls testing to ensure that the alternate storage and processing sites provide information security safeguards equivalent to that of the primary site.

In the self-assessment OPM conducted, this metric was assessed as *Defined* with the goal maturity level of *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 4, states the organization "Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site." NIST SP 800-53, Revision 4, also states the organization "Ensures that the alternate processing site provides information security safeguards equivalent to those of 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.

Recommendation 36 (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:

"Partially Concur. OPM takes every opportunity to use FedRAMP cloud service providers as more applications transition to the cloud. When OPM utilizes a FedRAMP cloud service provider, the CSP is expected to document the testing of controls. We will review the controls testing for OPM data centers."

OIG Comment:

The intent of the recommendation is to ensure that controls testing is performed and documented, either by OPM or a vendor, for alternate processing and storage sites. We agree that the cloud service provider is expected to perform and document the testing. However, during the course of this audit, we did not receive any evidence of control testing to ensure security safeguards for OPM's alternate processing and storage sites are equivalent to the primary sites.

Metric 65 - Communication of Recovery Activities

FY 2021 Maturity Level: 2 – Defined. OPM has defined the process of communicating results of recovery activities to stakeholders in policies and procedures. At the conclusion of a contingency plan test or significant service-impacting incident, results are to be communicated to stakeholders in the form of an after-action report. However, OPM is not adhering to this policy, as the self-assessment identified this weakness and OPM did not respond to a request for further information.

In the self-assessment OPM conducted, this metric was assessed as *Defined* with the goal maturity level of *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	Metric Maturity Level Definition	Domain Maturity Level	Function Maturity Level	U.S. OPM Overall Maturity Level
1 - Inventory of Major Systems and System Interconnections	3	Consistently Implemented	Risk Management Level 2: Defined	Identify Level 2: Defined	Agency Overall Level 2: Defined
2 - Hardware Inventory	1	Ad Hoc			
3 - Software Inventory	1				
4 - System Security Categorization	3	Consistently Implemented			
5 - Risk Policy and Strategy	2	Defined			
6 - Information Security Architecture	1	Ad Hoc			
7- Risk Management Roles, Responsibilities, and Resources	3	Consistently Implemented			
8 - Plan of Action and Milestones	2	Defined			
9 - Risk Communication	3	Consistently Implemented			
10 - Centralized Enterprise-wide Risk Tool	3				
11 - Risk Management Other Information -	n/a				
12 - SCRM Policies and Procedures	1	Ad Hoc	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	Consistently Implemented			
17 - Configuration Mgt. Roles, Responsibilities, and Resources	2	Defined	Configuration Management Level 2: Defined	Protect Level 2: Defined	
18 - Configuration Management Plan	2				
19 - Baseline Configurations	1	Ad Hoc			
20 - Security Configuration Settings	1				
21 - Flaw Remediation and Patch Management	2	Defined			
22 - Trusted Internet Connection Program	1	Ad Hoc			
23 - Configuration Change Control Management	3	Consistently Implemented			
24 - Vulnerability Disclosure Policy	2	Defined			
25 - Configuration Management Other Information	n/a	Consistently Implemented			
26 - ICAM Roles, Responsibilities, and Resources	1	Ad Hoc	Identify and Access Management Level 2: Defined		
27 - ICAM Strategy	1				
28 - Personnel Risk	3	Consistently Implemented			
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	Ad Hoc			
33 - Remote Access Connections	2	Defined			
34 - ICAM Other Information - Contractor Access Management	n/a	Consistently Implemented			
35 - Data Protection and Privacy Policies and Procedures	1	Ad Hoc	Data Protection and Privacy Level 2: Defined		
36 - Data Protection and Privacy Controls	2	Defined			
37 - Data Exfiltration Protection	4	Consistently Implemented			
38 - Data Breach Response Plan	2	Defined			
39 - Privacy Awareness Training	1	Ad Hoc			
40 - Other Information - Data Protection and Privacy	n/a	Consistently Implemented			
41 - Security Training Policies and Procedures	3	Consistently Implemented	Security Training Level 3: Consistently Implemented		
42 - Assessment of Workforce	2	Defined			
43 - Security Awareness Strategy	2				
44 - Tracking IT Security Training	4	Consistently Implemented			
45 - Tracking Specialized IT Security Training	4				
46 - Other Information - Security Training Program	n/a				
47- ISCM Strategy	2	Defined	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	2				
51 - ISCM Other Information	n/a	Consistently Implemented			
52 - Incident Response Policies, Procedures, Plans, and Strategies	4	Consistently Implemented	Incident Response Level 4: Managed and Measurable	Respond Level 4: Managed and Measurable	
53 - Incident Roles and Responsibilities	4				
54 - Incident Detection and Analysis	3				
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	Defined	Contingency Planning Level 2: Defined	Recover Level 2: Defined	
61 - Business Impact Analysis	2				
62 - Contingency Plan Maintenance	2				
63 - Contingency Plan Testing	2				
64 - Information System Backup and Storage	2				
65 - Communication of Recovery Activities	2				
66 - Contingency Planning Other Information	n/a	Consistently Implemented			

Appendix II - Status of Prior OIG Audit Recommendations

The table below outlines the current status of recommendations issued in the FY 2020 FISMA audit (Report No. 4A-CI-00-20-010, issued October 30, 2020).

Rec	Original Recommendation	Recommendation History	Current Status
1	We recommend that OPM improve the policies and procedures for defining system boundaries and classifying the systems in its environment.	Rolled forward from FY 2018	We support closure
2	We recommend that the OCIO ensure that all interconnection security agreements are valid and properly maintained.	Rolled forward from FY 2014	We support closure
3	We recommend that the OCIO ensure that a valid memorandum of understanding/agreement exists for every interconnection.	Rolled forward from FY 2014	We support closure
4	We recommend that OPM define the procedures for maintaining its hardware inventory.	New recommendation in FY 2019	**Open**: Rolled forward as Report 4A-CI-00-21-012 Recommendation 1
5	We recommend that OPM improve its system inventory by correlating the elements of the inventory to the servers and information systems they reside on.	Rolled forward from FY 2016	We support closure
6	We recommend that OPM define policies and procedures for a centralized software inventory.	Rolled forward from FY 2018	**Open**: Rolled forward as Report 4A-CI-00-21-012 Recommendation 2
7	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	**Open**: Rolled forward as Report 4A-CI-00-21-012 Recommendation 3
8	We recommend that the OCIO implement a process to ensure that only supported software and operating platforms are used within the network environment.	Rolled forward from FY 2016	We support closure
9	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 4A-CI-00-21-012 Recommendation 11
10	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 4A-CI-00-21-012 Recommendation 7
11	We recommend that the OPM Director ensure that the OCIO has sufficient resources to adequately operate, secure, and modernize agency IT systems. We also recommend that the agency hire a sufficient number of ISSOs to adequately support all of the agency's major information systems.	Rolled forward from FY 2016	We support closure
12	We recommend that OPM adhere to remediation dates for its POA&M weaknesses.	Rolled forward from FY 2016	**Open**: Rolled forward as Report 4A-CI-00-21-012 Recommendation 9

Rec	Original Recommendation	Recommendation History	Current Status
13	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	**Open**: Rolled forward as Report 4A-CI-00-21-012 Recommendation 10
14	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.	New recommendation in FY 2019	**Open**: Rolled forward as Report 4A-CI-00-21-012 Recommendation 5
15	We recommend that OPM identify and define the requirements for an automated enterprise-wide solution for tracking risks, remediation efforts, dependencies, risk scores, and management dashboards, and implement the automated enterprise-wide solution.	Rolled forward from FY 2017	We support closure
16	We continue to recommend that the OCIO develop a plan and timeline to enforce the new SDLC policy on all of OPM's system development projects.	Rolled forward from FY 2013	We support closure
17	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 4A-CI-00-21-012 Recommendation 12
18	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 4A-CI-00-21-012 Recommendation 13
19	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 4A-CI-00-21-012 Recommendation 14
20	We recommend that the OCIO conduct routine compliance scans against established baseline configurations for all OPM information systems. Note: This recommendation cannot be addressed until Recommendation 19 has been implemented.	Rolled forward from FY 2017	We support closure
21	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 4A-CI-00-21-012 Recommendation 15
22	We recommend that the OCIO conduct routine compliance scans against [the standard security configuration settings] for all servers and databases in use by OPM.	Rolled forward from FY 2017	We support closure
23	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 4A-CI-00-21-012 Recommendation 16

Rec	Original Recommendation	Recommendation History	Current Status
24	We recommend that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.	Rolled forward from FY 2014	We support closure
25	We recommend that the OCIO implement a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.	Rolled forward from FY 2014	We support closure
26	We recommend that the OCIO implement a process to apply operating system and third party vendor patches in a timely manner.	Rolled forward from FY 2014	We support closure
27	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 4A-CI-00-21-012 Recommendation 18
28	We recommend that OPM conduct an analysis to identify limitations in the current ICAM program in order to ensure that stakeholders have adequate resources (people, processes, and technology) to implement the agency's ICAM activities.	Rolled forward from FY 2017	We support closure
29	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 4A-CI-00-21-012 Recommendation 21
30	We recommend that OPM implement a process to capture and share lessons learned on the effectiveness of its ICAM policies, procedures, and processes to update the program.	Rolled forward from FY 2017	We support closure
31	We recommend that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.	Rolled forward from FY 2012	We support closure
32	We recommend that the OCIO maintain a centralized list of all contractors that have access to the OPM network and use this list to routinely audit all user accounts for appropriateness.	Rolled forward from FY 2016	We support closure
33	We recommend that OPM define the roles and responsibilities necessary for the implementation of the agency's privacy program.	Rolled forward from FY 2018	**Open**: Rolled forward as Report 4A-CI-00-21-012 Recommendation 24
34	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	**Open**: Rolled forward as Report 4A-CI-00-21-012 Recommendation 25
35	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 4A-CI-00-21-012 Recommendation 27
36	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 4A-CI-00-21-012 Recommendation 28
37	We recommend that all active systems in OPM's inventory have a complete and current Authorization.	Rolled forward from FY 2014	We support closure

Rec	Original Recommendation	Recommendation History	Current Status
38	We recommend that the performance standards of all OPM system owners be modified to include a requirement related to FISMA compliance for the information systems they own. At a minimum, system owners should be required to ensure that their systems have valid Authorizations.	Rolled forward from FY 2014	We support closure
39	We recommend that OPM ensure that an annual test of security controls has been completed for all systems.	Rolled forward from FY 2008	We support closure
40	We recommend that OPM evaluate qualitative and quantitative performance measures on the performance of its ISCM program once it can consistently acquire security assessment results, as referenced in Recommendation 39.	Rolled forward from FY 2017	We support closure
41	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 4A-CI-00-21-012 Recommendation 32
42	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	**Open**: Rolled forward as Report 4A-CI-00-21-012 Recommendation 33
43	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 Report 4A-CI-00-21-012 Recommendation 34
44	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 4A-CI-00-21-012 Recommendation 35
45	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 4A-CI-00-21-012 Recommendation 36

Appendix III

October 7, 2021

Memorandum For:	Eric Keehan Chief, Information System Audit Group Office of the Inspector General
Through:	Kellie Cosgrove Riley Chief Privacy Officer Office of Privacy and Information Management
From:	Guy Cavallo Chief Information Officer
Subject:	Office of Personnel Management Response to the Office of the Inspector General Federal Information Security Modernization Act Audit - FY 2021 (Report No. 4A-CI-00-21-012)

Thank you for the opportunity to provide comments to the Office of the Inspector General OIG) draft report regarding the Federal Information Security Modernization Act (FISMA) Audit for the U.S. Office of Personnel Management (OPM), Report No. 4A-CI-00-21-012. OIG's recommendations help to inform our continuous efforts to enhance data security and to protect the Federal workforce, Federal agencies, private industry, and the public.

We especially appreciate the revised approach to assess OPM's maturity level for the FISMA metrics. The agency's self-assessment of the metrics is a useful tool for OPM to take action to improve our security posture. We also 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. OPM and OIG will continue to work toward 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 16 of the OIG's 36 recommendations and partially concurs with 11 recommendations. More detailed responses to your recommendations and the planned corrective actions and expected timeframes, as appropriate, are provided below.

As OPM's new CIO and with support from the OPM's leadership, I have prioritized the staffing, management, and remediation of all audit findings by creating a new Audit Team within the OCIO Governance Organization. We will improve our ability to provide timely documentation of processes and evidence of consistent implementation going forward. A number of these audit findings would have been closed if we had provided procedures and documentation that are already in place. We will make sure that documentation is provided as we work together to improve OPM's IT operations and services.

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

Management's Response: We believe OPM is already in compliance with this recommendation. OPM has procedures to maintain the hardware inventory. We will review the procedures as necessary and will provide the documentation to OIG under separate cover.

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

Management's Response: Concur. OPM is documenting policies and procedures for a centralized software inventory. We will provide the policies and procedures to OIG once they are complete.

Recommendation 3 (Rolled forward from 2017): 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.

Management's Response: Concur. The Office of the Chief Information Officer (OCIO) has developed systems requirements specifications for an authoritative enterprise software registry that defines the standard data elements required to perform software management. Additionally, OCIO will continue to update the software inventory to include these standard data elements.

Recommendation 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.

Management's Response: We believe that OPM is in compliance with this recommendation. OPM instituted system categorization levels, business impact analyses, and uses risk information to prioritize the allocation of its resources. OPM is reviewing this practice and is formalizing the required evidence.

Recommendation 5 (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: Partially Concur. OPM has risk assessments for some systems, but not all. OPM will review the risk assessments for each major system and will take steps to ensure that control tests are included, where they are not already included. OPM will provide evidence to OIG once the review is complete.

Recommendation 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.

Management's Response: We believe that OPM is in compliance with this recommendation. OPM created a cybersecurity risk register, periodically reviews the register, and shares lessons learned with risk owners. OPM will gather and provide evidence of the register and risk management practices to OIG under separate cover.

Recommendation 7 (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 will update the enterprise architecture to include the necessary information security architecture elements. Additionally, OCIO is hiring an enterprise architect to map IT assets and to drive business strategy through information technology.

Recommendation 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.

Management's Response: We believe that OPM is in compliance with this recommendation. OPM uses a risk-based approach when allocating resources for cybersecurity risk management activities.

Recommendation 9 (Rolled forward from 2016): We recommend that OPM adhere to remediation dates for its Plan of Action and Milestone (POA&M) weaknesses.

Management's Response: Partially Concur. OPM has instituted metrics and processes to identify, monitor, and track the completion of Plan of Action & Milestones (POA&Ms). We will re-baseline when slippage occurs.

Recommendation 10 (Rolled forward from 2017): 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 should be maintained to track the schedule variance).

Management's Response: Partially Concur. OPM has instituted metrics and processes to identify, monitor, and track the completion of Plan of Action & Milestones (POA&Ms). We will re-baseline when slippage occurs.

Recommendation 11 (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 will take the steps necessary to address supply chain risk management requirements.

Recommendation 12 (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. OPM recently awarded a technology contract to develop enterprise configuration management standards and the automated processes to implement and maintain the standards.

Recommendation 13 (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. OPM recently awarded a technology contract to develop enterprise configuration management standards and the automated processes to implement and maintain the standards.

Recommendation 14 (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 has configuration settings for recent implementations. The configuration settings will be presented to OIG under separate cover. We are developing and implementing standard configuration settings for legacy and older OPM information systems. We will continually implement the standard configuration settings for new deployments of operating platforms through enhancements to the Enterprise Configuration Management process.

Recommendation 15 (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. The CIO has determined that the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) will be the primary baseline for all OPM configuration settings of information systems. The DISA STIG will be modified to meet OPM's non-military requirements. Those modifications will be documented and provided to OIG under separate cover. We patched older/legacy systems to ensure standard security configuration settings are consistently updated.

Recommendation 16 (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 is using standard security configuration settings based on DISA's STIG for all operating platforms. We will request approval for deviations and document deviations from the standard security configuration settings in the system configuration baseline.

Recommendation 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 OPM policy.

Management's Response: Partially Concur. OPM is in compliance for end-user devices and servers. We will review the target timeframe to apply patches to the mainframes to confirm that we are conforming to a 30 day window.

Recommendation 18 (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: Partially Concur. The new practice that servers be included in the scan repository. We will document the new practice and provide evidence to OIG.

Recommendation 19: We recommend that OPM establish an agency-wide TIC program to manage and maintain its external agency connections.

Management's Response: Non-Concur. OPM TIC is currently located in the Boyers data center.

Recommendation 20: We recommend that OPM create a charter to govern the roles and responsibilities of its ICAM office's governance body.

Management's Response: Concur. OPM is taking an enterprise approach to Identity, Credential, and Access Management (ICAM). The Chief Technology Officer (CTO) came onboard in late FY 2021 and will lead the ICAM strategy. OPM will aim to create a charter to govern the roles and responsibilities of the ICAM governance body.

Recommendation 21 (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. The CIO has applied an enterprise view to ICAM. The CTO recently came on board and is responsible for the ICAM strategy. The CTO will coordinate with the CISO and EIS to review current ICAM practices, identify gaps, and develop action plans and milestones. We aim to complete the analysis in Q2 of FY 2022. We will provide the analysis and milestones to OIG once they are complete.

Recommendation 22: We recommend that OPM define its process for provisioning, managing, and reviewing privileged accounts.

Management's Response: We believe that OPM is in compliance with this recommendation.

We are provisioning, managing, and reviewing privileged accounts in compliance with the Continuous Diagnotics and Mitigation (CDM) requirement.

Recommendation 23: We recommend that OPM routinely review remote connection event logs in accordance with its Information System Monitoring Policy.

Management's Response: Non-Concur. OPM is in compliance with this recommendation and routinely review our remote connection event logs.

Recommendation 24 (Rolled forward from 2018): We recommend that OPM define the roles and responsibilities necessary for the implementation of the agency's privacy program.

Management's Response: Partially Concur. The Office of Privacy and Information Management (OPIM) and its roles and responsibilities were approved and established by the former Acting Director as a stand-alone office in February 2019. Artifacts have been provided to the OIG over the succeeding years to document OPIMs functions and duties. As resources permit, we will continue to develop and reinforce these roles and responsibilities at the Agency.

Recommendation 25 (Rolled forward from 2018): We recommend that OPM develop its privacy program by creating the necessary plans, policies, and procedures for the protection of PII.

Management's Response: Partially Concur. OPIM has established and communicated our policies, templates, and guidance regarding the privacy program plan through a wide range of tools including positioning documents and information on THEO for our employees. We have established a public-facing OPM web page devoted to privacy including our published Systems of Records Notices, Privacy Impact Assessments, and Computer Matching Agreements. The web pages are updated regularly as new documents are prepared. We continue to guide program offices and the CIO offices on Privacy Threshold Analysis (PTA) and Privacy Impact Assessments (PIA) compliance documents. We collaborated with the CIO in preparing the privacy awareness module on protecting Personally Identifiable PII for the 2021 IT Security and Privacy Awareness mandated training. We will be updating the previously published OPM Security and Privacy Policy Handbook or reasonable alternatives to reflect the current state of privacy policy.

Recommendation 26: We recommend that OPM implements 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.

Management's Response: Partially Concur. OPM has defined and communicated its controls to protect sensitive information in its environment. The controls include the use of FIPS validated encryption of PII and other agency sensitive data both at rest and in transit, controls to prevent and detect untrusted removable media, and controls related to the destruction or reuse of media containing PII or other sensitive agency data.

Recommendation 27 (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 Data Breach Response Plan was issued in 2017. OPIM will update the Data Breach Response Plan and develop and implement an annual table-top exercise to test the plan as resources permit during the next fiscal year.

Recommendation 28 (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. OPIM has conducted role-based training for supervisors on privacy via the bi-weekly supervisory meetings held by HR. We will work to catalog additional role-based training across other positions and aim to provide role-based training to individuals in those positions as time and resources permit.

Recommendation 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.

Management's Response: We believe that OPM is in compliance with this recommendation. We have performed the workforce assessment. We have also performed the gap analysis to identify the skills gaps and training needs.

Recommendation 30: We recommend that OPM consistently capture information to show quantitative and qualitative data for its ongoing security assessments.

Management's Response: We believe that OPM is in compliance with this recommendation.

Recommendation 31: We recommend that OPM complete its development of profiling techniques on its networks and systems to more effectively detect security incidents.

Management's Response: Partially Concur. We have implemented profiling techniques for some enterprise systems. We continue to expand the techniques to other systems.

Recommendation 32 (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. OPM is performing a gap analysis and updating the contingency plans to modify the requirements.

Recommendation 33 (Rolled forward from FY 2017): 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.

Management's Response: Concur. OPM will reflect the agency-wide Business Impact Analysis (BIA) results in the system-level contingency plans that we are updating.

Recommendation 34 (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. OCIO has contingency plans for systems that were implemented recently. We will provide those plans under separate cover. We will review the contingency plans for older/legacy systems to verify that they are up to date. We will conduct gap analysis and annual reviews for recent and older/legacy systems.

Recommendation 35 (Rolled forward from 2008): We recommend that OPM test the contingency plans for each system on an annual basis.

Management's Response: Concur. The OCIO will conduct a gap analysis. Once the gap analysis is complete, OPM will test the contingency plans for each system on an annual basis with each system's Program Management Office including the system owners and authorizing officials.

Recommendation 36 (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: Partially Concur. OPM takes every opportunity to use FedRAMP cloud service providers as more applications transition to the cloud. When OPM utilizes a FedRAMP cloud service provider, the CSP is expected to document the testing of controls. We will review the controls testing for OPM data centers.

I appreciate the opportunity to respond to the draft report. I also look forward the continuous collaboration to enhance data security. Please contact me if you have questions or need additional information.

cc:

Anne Harkavy
Chief of Staff

Margaret Pearson
Acting Chief Financial Officer

Mark W. Lambert
Associate Director, Merit System Accountability and Compliance

Janet L. Barnes
Director, Internal Oversight and Compliance

Melvin Brown
Acting Deputy Chief Information Officer

Larry Allen
Acting Associate Chief Information Officer, IT Strategy & Policy

Cord E. Chase
Chief Information Security Officer

Lynn Eisenberg
General Counsel

Technical Comments on U.S. Office of Personnel Management's Security Assessment and Authorization Methodology, Report No. 4A-CI-00-21-012, dated September 17, 2021

On page 14, under *Metric 8 – Plan of Action and Milestones*, the following reference is made:

We analyzed all 887 open POA&Ms located in the GRC tool. Our analysis identified that over 60% of the POA&Ms were overdue. More specifically, as of August 23, 2021, we noted the following:

- *34 % of POA&Ms have not been updated in over 12 months;*
- *11 % of POA&Ms have not been updated in 7 – 12 months;*
- *2% of POA&Ms have not been updated in 4-6 months; and*
- *15% of POA&Ms have not been updated in 1-3 months.*

After reviewing the POA&M extract used for this analysis, OPM has the following comments:

The POA&M extract that forms the basis of the evaluation includes POA&Ms for systems that are decommissioned or that belong to DCSA. These POA&Ms are not a part of OPM's inventory. The extract also does not include key fields to accurately extract the POA&Ms from the list without introducing human error. Thus, we were not able to provide an exact comparison and correction of what the numbers should be versus the content of the report.

The POA&M values and percentages make comparisons to POA&Ms that are not open. The initial and draft stages (and their corresponding MRB review stages) in the POA&M process represent planning steps. They have not been finalized/approved in the Scheduled Completion Date and Expected Completion Date values. OPM considers that when a POA&M is submitted for closure, it has reached its resolution target.
POA&Ms in after open stages, including Awaiting MRB Closure Review and Awaiting Audit Liaison View, POA&Ms are not measured in the evaluation of open POA&Ms.

"Overdue" POA&Ms should not include records in after open stages.

The POA&M update values and percentages are based on the Scheduled Completion Date. The Scheduled Completion Date is the initial date recorded for a POA M and does not reflect the current target date to complete the milestones. It is retained to evaluate schedule variance as necessary (refer to Recommendation 10). The Expected Completion Date is updated when POA&Ms are updated. The Scheduled Completion Date is not updated when POA&Ms are updated. Using the Scheduled Completion Date to identify overdue POA&Ms will not produce an accurate list of overdue POA Ms.

Below is a description of the OPM's current POA&M status as of 11:40am on September 30, 2 021 for the purpose of comparison.

- Total Open POA&Ms: 564
- Total Open POA&Ms past the Expected Completion Date: 71 (13%)
- Total Open POA&Ms past the Expected Completion Date, last updated over 365 days ago: 7 (1%)
- Total Open POA&Ms past the Expected Completion Date, last updated between 180 days and 365 days ago: 16 (3%)
- Total Open POA&Ms past the Expected Completion Date, last updated between 90 days and 180 days ago: 36 (6%)
- Total Open POA&Ms past the Expected Completion Date, last updated between 30 days and 90 days ago: 4 (1%)

Report Fraud, Waste, and Mismanagement

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

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

By Phone: Toll Free Number: 877) 499-7295
Washington Metro Area 202) 606-2423

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