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 2019

Report Number 4A-CI-00-19-029
October 29, 2019

EXECUTIVE SUMMARY

Federal Information Security Modernization Act Audit - Fiscal Year 2019

Report No. 4A-CI-00-19-029 **October 29, 2019**

Why Did We Conduct the Audit?

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

What Did We Audit?

The OPM Office of the Inspector General has completed a performance audit of OPM's general FISMA compliance efforts in the areas defined in DHS's guidance and the corresponding reporting instructions. Our audit was conducted from April through September 2019 at OPM headquarters in Washington, D.C.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

The Fiscal Year (FY) 2019 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 eight "domain" areas and the modes (i.e., the number that appears most often) of the domain scores are used to derive the agency's overall cybersecurity score. In FY 2019, OPM's cybersecurity maturity level is measured as "2 - Defined." While continued improvements in maturity are necessary, OPM made progress in FY 2019, closing eight prior recommendations.

The following sections provide a high-level outline of OPM's performance in each of the eight domains from the five cybersecurity framework function 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 system interconnections, hardware assets, and software.

Configuration Management – OPM continues to develop baseline configurations and approve standard configuration settings for its information systems. The organization is also working to establish routine audit processes to ensure that its systems maintain compliance with the established configurations.

Identity, Credential, and Access Management (ICAM) – OPM is continuing to develop its agency ICAM strategy, and acknowledges a need to implement an ICAM program. However, OPM still does not have sufficient processes in place to manage contractors in its environment.

Data Protection and Privacy – OPM has implemented some controls related to data protection and privacy. However, there are still resource constraints within OPM's Office of Privacy and Information Management that limit its effectiveness.

Security Training – OPM has implemented an information technology (IT) security training strategy and program, and has performed a workforce assessment but still needs to identify gaps in its IT security training program.

Information Security Continuous Monitoring (ISCM) – OPM has established many of the policies and procedures surrounding ISCM, but the organization has not completed the implementation and enforcement of the policies. OPM also continues to struggle with conducting a security controls assessment on all of its information systems. Routine controls testing has been an ongoing weakness at OPM for over a decade.

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 struggle with maintaining its contingency plans as well as conducting contingency plan tests on a routine basis. Contingency plan testing has been an ongoing weakness at OPM for over a decade.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
BIA	**Business Impact Analysis**
CDM	**Continuous Diagnostics and Mitigation**
CM	**Configuration Management**
DHS	**U.S. Department of Homeland Security**
ECM	**Enterprise Change Management**
FICAM	**Federal Identity, Credential, and Access Management**
FISCAM	**Federal Information System Controls Audit Manual**
FISMA	**Federal Information Security Modernization Act**
FY	**Fiscal Year**
ICAM	**Identity, Credential, and Access Management**
IG	**Inspector General**
ISCM	**Information Security Continuous Monitoring**
ISSO	**Information System Security Officer**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
OCFO	**Office of the Chief Financial Officer**
OCIO	**Office of the Chief Information Officer**
OIG	**Office of the Inspector General**
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**
SAOP	**Senior Agency Official for Privacy**
SCRM	**Supply Chain Risk Management**
SDLC	**Systems Development Life Cycle**
SP	**Special Publication**

TABLE OF CONTENTS

I. BACKGROUND

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

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

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

To assist agencies and 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) 2019 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 2019 FISMA IG Reporting Metrics utilizing a maturity model evaluation system derived from the National Institute of Standards and Technology (NIST) Cybersecurity Framework. We designed our audit and reporting approaches in accordance with the issued guidance.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

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

We also followed-up on outstanding recommendations from prior FISMA audits, and performed audits focused on six of OPM's major information systems – the Enterprise Human Resources Integration Data Warehouse, the Federal Financial System, the Consolidated Business Information System, the Macon General Support System, the Enterprise Server Infrastructure General Support System, and the Local Area Network/Wide Area Network General Support System.

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 2019.

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 OPM appropriately designed and implemented the internal controls. As appropriate, we conducted compliance tests using judgmental samples to determine the extent to which established controls and procedures are functioning as required.

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 2019 IG FISMA Reporting Metrics;
- OPM Information Technology Security and Privacy Policy Handbook;
- OPM Information Technology Security FISMA Procedures;
- OPM Security Assessment and Authorization Guide;
- OPM Plan of Action and Milestones Standard Operating Procedures;
- OMB Circular A-130, Managing Information as a Strategic Resource;
- OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive 12;

- OMB Memorandum M-19-17: Enabling Mission Delivery through Improved Identity, Credential, and Access Management;
- P.L. 107-347, Title III, Federal Information Security Management Act of 2002;
- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST Special Publication (SP) 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy;
- NIST SP 800-39, Managing Information Security Risk – Organization, Mission, and Information System View;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60, Volume 1, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories;
- NIST SP 800-60, Volume 2, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories;
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information;
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems;
- Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems;
- Federal Cybersecurity Workforce Assessment Act of 2015;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;
- Federal Information System Controls Audit Manual (FISCAM); and

- Other criteria as appropriate.

The OPM Office of the Inspector General (OIG), established by the Inspector General Act of 1978, as amended, performed the audit from April through September 2019 in OPM's Washington, D.C. office.

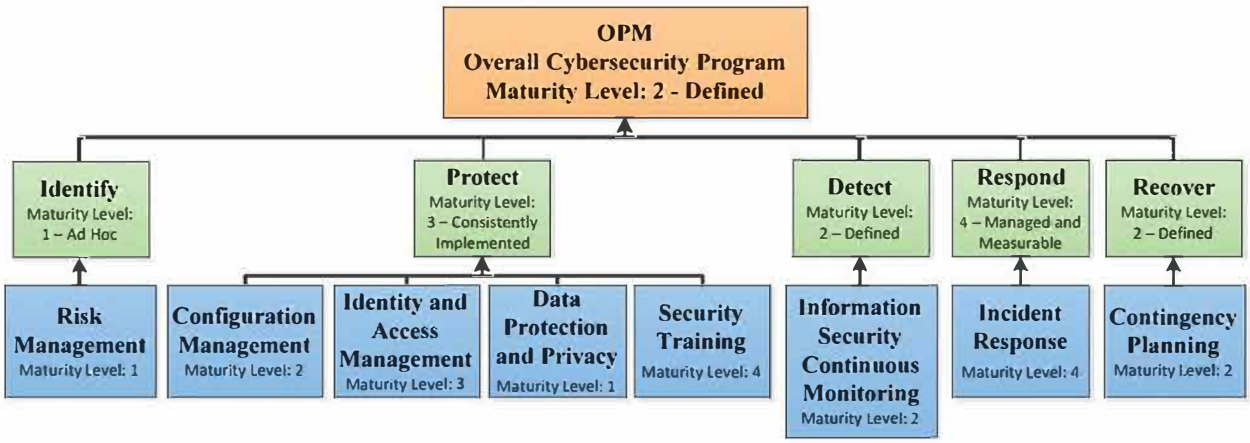
COMPLIANCE WITH LAWS AND REGULATIONS

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

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. INTRODUCTION AND OVERALL ASSESSMENT

The FY 2019 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 eight "domains" under the function areas. These eight domains are broad cyber security control areas used to assess the effectiveness of the information security policies, procedures, and practices of the agency. Each domain is comprised of a series of individual metrics, which are the specific controls that we evaluate and test when assessing the agency's cybersecurity program. Each metric receives a maturity level rating of 1-5. The chart below outlines the overall "2 – Defined" maturity level of OPM's cybersecurity program.

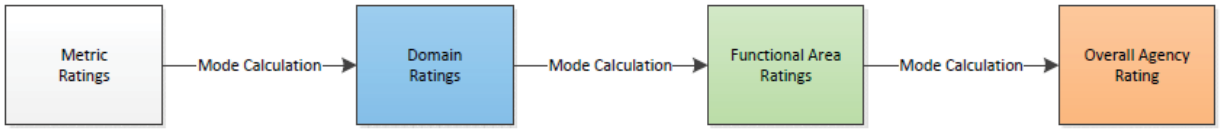


The following table outlines the description of each maturity level rating, as defined by the FY 2019 IG FISMA Reporting Metrics:

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measureable	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.

The mode (i.e., the number that appears most often) from the maturity levels of each individual metric is used to determine the corresponding domain rating and in the event of a tie between maturity levels the higher level is used. Similarly, the mode from the domain ratings assigns the function area rating. We calculated the overall agency rating using the same methodology. However, IGs have discretion in the function and agency ratings to consider agency specific factors, especially in the event of a tie between the domain or functional area maturity ratings.



The remaining sections of this report provide the detailed results of our audit. Information Security Governance and Security Assessment and Authorizations (Authorization) did not directly map to the domains, but warranted separate discussions in prior reports as both substantially hindered the agency's performance in prior years. We are no longer highlighting these areas separately and will be addressing them in the corresponding FY 2019 FISMA IG Reporting Metrics. Sections B through I 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 "1 – Ad-hoc."**

Metric 1 – Inventory of Major Systems and System Interconnections

FY 2019 Maturity Level: 1 – Ad-hoc. OPM policy requires that the agency keep a major system inventory, to include system interconnections.[1] While the agency has established a central

[1] System interconnections are documented in memoranda of understanding/agreements and interconnection security agreements.

repository for its system inventory, agency procedures require that system boundaries be defined before the system can be properly classified. At that point the system and interconnections should be added to the system inventory and undergo the Authorization process.

One of the first steps in the Authorization process is defining the Authorization or system boundary. OPM has historically not fully defined its existing system boundaries. Management of OPM systems remains decentralized, with program offices maintaining system ownership and non-technical individuals assigned responsibility for critical areas of system security – including defining information system boundaries and approving security controls. The current policy states that system owners are responsible for documenting system boundaries but a procedure for deciding what is or is not a part of a given system does not exist. The lack of a requirement to determine what is and is not part of a given system cascades into a number of other metrics, (Metric 2 - Hardware Inventory; Metric 3 - Software Inventory; Metric 6 - Information Security Architecture; and Metric 13 - System Development Life Cycle, below). In each case, OPM struggles to identify and maintain the information about what resides in its environment. Consistently implemented and documented system boundaries combined with properly correlated component inventories would result in less risk of improperly classified systems.

NIST SP 800-53, Revision 4, requires that an organization "develops and maintains an inventory of its information systems." Furthermore, NIST requires an organization "Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated . . ." and regularly reviews, updates, and authorizes each connection.

Failure to consistently apply system boundaries increases the risk that system components are not all subject to the required security process. In addition, failure to document and approve all systems and interconnections increases the risk that information systems will improperly contain, share, or fail to protect sensitive information.

Recommendation 1 (Rolled forward from 2018)

We recommend that OPM improve the policies and procedures for defining system boundaries and classifying the systems in its environment.

OPM Response:

"We concur with the recommendation. OPM considers its policy to be sufficient to meet the intent of the finding as described in the report. However, we are in the process of making revisions to our procedures to align with enhancements to NIST SP 800-37[,] Revision 2, which will affect how we execute system boundary definitions and system classifications."

OIG Comment:

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

This statement applies to all subsequent recommendations in this audit report that the OCIO agrees to implement.

Recommendation 2 (Rolled forward from 2014)

We recommend that the OCIO ensure that all interconnection security agreements are valid and properly maintained.

OPM Response:

"We concur with the recommendation. Early in the fiscal year, several Information System Security Officers (ISSOs) were brought on board with additional contract ISSOs expected to join in the coming months. The OPM [Chief Information Officer] completed an ISSO service requirement gap analysis which was a critical component of [the] OCIO['s] efforts to obtain the appropriate funding. [The] OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs will be able to address the development and maintenance of interconnection security agreements."

Recommendation 3 (Rolled forward from 2014)

We recommend that the OCIO ensure that a valid memorandum of understanding/agreement exists for every interconnection.

OPM Response:

"We concur with the recommendation. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. The OCIO completed an ISSO service requirement gap analysis which was a critical component of [the] OCIO['s] efforts to obtain the appropriate funding. [The] OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. The ISSO service model developed in 2019 addresses the development and maintenance of memorandum of understandings/agreements which we anticipate will assist in meeting this metric."

Metric 2 – Hardware Inventory

OPM does not have documented procedures for maintaining its hardware inventory.

FY 2019 Maturity Level: 1 – Ad-hoc. OPM has defined a policy requiring that hardware assets be inventoried, and implemented a software tool to store this information. Despite OPM not having documented procedures to maintain an inventory, the OCIO's hardware inventory does include many of the required elements. However, many assets are incomplete (e.g., missing serial numbers) or include inaccurate information (e.g., incorrect location). In addition, the hardware inventory does not contain information to associate hardware components to the major system(s) that they support.

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 a current inventory increases the risk that unmaintained or outdated components reside in the environment, increasing the risk of potential compromise. 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 4

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

OPM Response:

"We concur with the recommendation. In FY 2020, we plan to update procedures for maintaining the OPM hardware inventory."

Recommendation 5 (Rolled forward from 2016)

We recommend that OPM improve its system inventory by correlating the elements of the inventory to the servers and information systems they reside on.

OPM Response:

"We concur with the recommendation. OPM plans to meet this requirement by leveraging toolsets provided by the [DHS] Continuous Diagnostics and Mitigation (CDM) program. OPM is in the processing of entering FISMA system boundaries into its CDM tool and is

planning to import this data into the Governance, Risk Management, and Compliance . . . tool."

Metric 3 – Software Inventory

FY 2019 Maturity Level: 1 – Ad-hoc. OPM has defined a policy requiring software components be inventoried in an agency centralized inventory. OPM does not have documented procedures to maintain an inventory but did provide a list of software. However, this list only included application names and version numbers. There was no information about where the software is located, how many copies exist, the responsible parties, or licensing. In addition, there were instances of unsupported software listed in the inventory.

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 6 (Rolled forward from 2018)

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

Note: While OPM has defined a policy requiring a centralized software inventory, this recommendation remains open, as the agency has not developed the procedures.

OPM Response:

"We concur with the recommendation. We plan to expand the OPM Enterprise Change Management (ECM) program, enhance the software inventory, and evaluate the associated reporting and procedures."

Recommendation 7 (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:

"We concur with the recommendation. We will continue to improve upon the agency's enterprise architecture in FY 2020, specifically regarding the agency software inventory."

Recommendation 8 (Rolled forward from 2016)

We recommend that the OCIO implement a process to ensure that only supported software and operating platforms are used within the network environment.

OPM Response:

"We concur with the recommendation. Currently, any time new software is installed on a device, OPM is able to detect the installation. The ECM program will be enhanced to require approval through the ECM process for software installation. We are also actively developing plans to remove unsupported software and operating platforms from the network."

Metric 4 – System Security Categorization

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM has implemented policies and procedures for categorizing its information and information systems that follow Federal Information Processing Standard 199 and NIST SP 800-60 guidance. This includes the identification of the agency's high value assets and consideration of the system categorization when selecting, implementing, and monitoring controls.

Metric 5 – Risk Policy and Strategy

FY 2019 Maturity Level: 1 – Ad-hoc. OPM's OCIO has defined policies for assessing and reporting IT-related risks. OPM's Risk Management Council serves as the primary risk executive function and is responsible for the agency-wide risk management program. The council meets regularly and has defined a risk profile for OPM. The OCIO has been delegated the responsibility of managing cyber security risks and has documented a specialized risk strategy for this purpose.

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."

However, OPM is not yet including supply chain risk management (SCRM) in its risk management processes. The agency's current risk profile, strategies, and policies do not specifically incorporate supply chain risks. OPM is awaiting further guidance from OMB and has not yet defined a plan to comply with the requirements of this act.

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 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.

OPM Response:

"We concur with the recommendation. OPM will continue to follow government-wide guidance and standards to address this recommendation."

Metric 6 – Information Security Architecture

OPM's enterprise architecture has not been updated since 2008.

FY 2019 Maturity Level: 1 – Ad-hoc. The OMB *[Federal Enterprise Architecture] Practice Guidance* states that an enterprise architecture "describes the current and future state of the agency, and

lays out a plan for transitioning from the current state to the desired future state." OPM's enterprise architecture has not been updated since 2008 despite significant changes to its environment and plans, and does not support the necessary integration of an information security architecture. OPM has not documented an Information Security Architecture. In FY 2018, the agency contracted for enterprise architecture services, however, finalized architectures still do not exist.

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 have 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 10 (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:

"We concur with the recommendation. We will continue to update the enterprise architecture including the necessary information system security architecture. In FY [2019] we began the process of updating the enterprise architecture."

Metric 7 – Risk Management Roles, Responsibilities, and Resources

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM has defined the necessary roles and responsibilities of stakeholders in its risk management program. This includes the role of the Risk Management Council and the OCIO, as well as defining the responsibilities of information system owners, information security staff, and authorizing officials. The Risk Management Council has created an agency risk profile and strategy for OPM.

OPM's Risk Management Strategy delegates Cybersecurity risk management to the IT Security/Policy Office in the OCIO. In FY 2019, the OCIO designed a new chargeback model for the ISSO program to establish the financial resources to support an adequate number of ISSOs. This model is slated to be implemented in FY 2020. Another part of the plan to mitigate resource issues is to use contractors to fill some of the vacant roles.

Despite these steps, currently the OCIO continues to struggle to address long-standing recommendations. OPM has defined policies that require annual contingency plan updates, contingency plan testing, regular system risk assessments, and continuous monitoring. However, the agency has not been able to complete the annual requirement to test the security controls and contingency plans of all of its major information technology systems since 2008. OPM has not made sufficient progress in adopting a mature continuous monitoring program.

Failure to have a mature and consistent overall 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 11 (Rolled forward from 2016)

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.

OPM Response:

"We concur with the recommendation. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. The OCIO completed an ISSO service requirement gap analysis[,] which was a critical step to obtain the appropriate resources. [The] OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model."

Metric 8 – Plan of Action and Milestones

FY 2019 Maturity Level: 2 – Defined. The Plan of Action and Milestones (POA&M) is a tool used to track known weaknesses in information system controls and the corresponding remediation efforts. Previous FISMA audits identified serious issues with the OPM POA&M process, primarily related to system owners not meeting the self-assigned scheduled completion dates for remediating weaknesses. During June 2019, OPM performed a POA&M sprint to focus

on the long-standing issues with POA&M documentation. OPM POA&M documentation has improved over prior years; however, we still noted the following issues as of August 2019:

- 33 percent were more than 30 days overdue;
- 23 percent were more than 120 days overdue; and
- 45 percent are in draft or initial status (some since 2012).

The process of tracking, updating, and closing POA&Ms is key to understanding the changing level of risk that a system faces and how that system affects the risks of the agency. Without up-to-date POA&M information, the agency cannot make effective risk-based decisions and efficiently allocate resources to address risks.

Failure to remediate known weaknesses increases the risk that agency systems will be vulnerable to attack.

Recommendation 12 (Rolled forward from 2016)

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

OPM Response:

"We concur with the recommendation. The OCIO prioritized POA&M remediation and management in FY [2019], recently conducting a POA&M sprint, for example. Efforts to maintain remediation details will continue post-sprint through the use of a new POA&M reporting process and enhanced tools to help us manage the enterprise inventory of POA&Ms. Since we completed our sprint, we have been able to close 36 percent of POA&Ms across the board."

Recommendation 13 (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:

"We concur with the recommendation. The OCIO has prioritized POA&M remediation and management in FY [2019], recently conducting a POA&M sprint as previously noted. Efforts to maintain remediation details will continue post-sprint through the use of a new POA&M reporting process and enhanced tools to help us manage the enterprise inventory of POA&Ms. We have improved the POA&M process across the remediation stages with the speed by which they are reviewed and processed. This improvement in speed of review and processing helps to prevent POA&Ms from missing remediation deadlines."

Metric 9 – System Level Risk Assessments

Agency officials may not have all of the necessary risk information to authorize systems appropriately.

FY 2019 Maturity Level: 2 – Defined. OPM policy requires routine risk assessments for each system as part of the Authorization process. OPM has defined the policies and procedures for conducting test of controls and the associated risk assessments for individual information systems. We reviewed risk assessment documentation for all of OPM's major systems. We identified at least one significant problem with 70 percent of the assessments. Not documenting the Authorizing Official's review and approval was the most common issue identified. In addition, we noted other issues with completeness and documentation. Controls testing and risk assessments are a key part of the Authorization process, and the problems we found indicate that Authorizing Officials may not have all of the necessary risk information when granting an Authorization.

OPM policy requires, "All controls selected by the system . . . are assessed" and "an assessment of the risk to the system for each weakness is performed."

Failure to assess all system controls and system risks increases the possibility that weaknesses will not be identified in the system controls or that the information will not be incorporated when determining whether a system is authorized to operate.

Recommendation 14 (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:

"We concur with the recommendation. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. The OCIO completed an ISSO service requirement gap analysis which was a critical step to obtain the appropriate resources. [The] OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs will be able to improve the risk assessment metric."

Metric 10 – Risk Communication

FY 2018 Maturity Level: 3 – Consistently Implemented. The timely communication of risk information is critical to an effective risk management program. OPM has implemented policies and procedures to communicate information about risks, both across the agency and externally, as required. The OCIO integrates this communication into the Authorization, vulnerability management, and continuous monitoring processes. As OPM continues to improve in these areas, the timely communication of risk information will continue to play a critical role in working to protect OPM's systems and infrastructure.

Metric 11 – Contracting Clauses

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM policy mandates the use of specific contracting language and service level agreements to ensure contractors meet both Federal and OPM standards. This language includes information privacy and security requirements, such as protection, detection, and reporting of information. This ensures that contractor systems and services are implementing required controls, and that OPM receives the information it needs to monitor and assess any risks. For both internal and external systems, OPM uses the same process to evaluate that controls are working properly and effectively to reduce risk.

Metric 12 – Centralized Enterprise-wide Risk Tool

FY 2019 Maturity Level: 1 – Ad-hoc. OPM does not have a system or tool to view centralized enterprise-wide risk information. The Risk Management Council has the responsibility of understanding and determining risk at the agency level, but this will be both a monumental task and highly inefficient without centralized storage of agency-wide risk information. In FY 2018, OPM began the preliminary effort to define the system requirements by documenting high-level system mandates (i.e., the Federal and agency requirements for security and processing standards). However, in FY 2019 the agency made no further progress.

NIST SP 800-39 gives four responsibilities to the risk executive function that would require an agency-wide view of risk:

- "Manage threat and vulnerability information with regard to organizational information systems and the environments in which the systems operate;

- Establish organization-wide forums to consider all types and sources of risk (including aggregated risk);

- Determine organizational risk based on the aggregated risk from the operation and use of information systems and the respective environments of operation;" and

- "Develop a greater understanding of risk with regard to the strategic view of organizations and their integrated operations . . . ."

Failure to implement an automated enterprise risk management tool increases the risk that information is not captured, current, and/or is not being assessed in aggregate.

Recommendation 15 (Rolled forward from 2017)

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.

OPM Response:

"We concur with this recommendation. OPM developed requirements for an automated Enterprise Risk Management . . . solution. However, [the Office of the Chief Financial Officer (OCFO)] was unable to finalize requirements, conduct acquisition activities, and begin deployment of an [Enterprise Risk Management] solution across OPM programs as enterprise risk management staff was reprioritized to work on transition-related priorities. [The] OCFO was also unable to acquire an enterprise risk management automated tool in FY 2019 due to the lapse in funding and reprioritization. It was and it is still [the] OCFO's goal to implement an automated solution to manage its enterprise risk management program. In FY 2020, the [Chief Financial Officer] will direct Risk Management and Internal Control . . . to update its plan for the implementation of an [Enterprise Risk Management] solution post transition-related priorities and budget uncertainties."

Metric 13 – Risk Management Other Information - System Development Life Cycle

OPM last updated its System Development Life Cycle (SDLC) policy in 2013, and to date it is still not actively enforced for all IT projects. As noted in the FY 2017 OIG FISMA audit report, OPM's long history of troubled system development projects further emphasizes the need for OPM to develop a plan to enforce its SDLC policy. As of FY 2019, OPM has not enforced the SDLC policy at an enterprise level.

FISCAM states that "The SDLC should provide a structured approach for identifying and documenting needed changes to computerized operations; assessing the costs and benefits of various options, including the feasibility of using off-the-shelf software; and designing, developing, testing, and approving new systems and system modifications."

Failure to maintain an effective SDLC methodology increases the risk that OPM will waste resources on system development projects that will not meet the needs and/or requirements of the agency. It also increases the likelihood that OPM does not adequately build IT security controls into a new system during the development process, resulting in a potentially insecure system.

Recommendation 16 (Rolled forward from 2013)

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.

OPM Response:

"We concur with the recommendation. We recognize the need to enforce its SDLC policy on all IT projects and plan to implement corrective actions when we can support such activities weighed against other priorities."

C. 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. OPM did not improve its CM program in FY 2019. Furthermore, we have identified additional areas for improvement in this domain. 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 14 – Configuration Management Roles, Responsibilities, and Resources

FY 2019 Maturity Level: 2 – Defined. OPM has policies and procedures in place defining CM stakeholders and their roles and responsibilities. However, OPM has indicated that it does not have adequate resources (people, processes, and technology) to manage its CM program effectively.

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

Failure to have adequate resources to manage CM operations increases the risk of improperly configured devices on the network and malicious attacks.

Recommendation 17 (Rolled forward from FY 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:

"We concur with the recommendation. We will work to define and obtain the resource requirements to improve the configuration management program."

Metric 15 – Configuration Management Plan

FY 2019 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, OPM has not established a process to document lessons learned from its change control process.

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 18 (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:

"We do not concur with this recommendation[,] as it is dependent upon the closure of an associated recommendation. Given the gap analysis to be conducted for [R]ecommendation 17, which will include best practices based on lessons learned and other factors, this recommendation cannot be countenanced until maturation of the CM program implementation and is thus not timely or appropriate."

OIG Comment:

Documenting lessons learned is a common requirement in many of the FISMA domains and in many process improvement methodologies. Documenting lessons learned is separate from the intent of Recommendation 17, which focuses on the fact that OPM's current CM program does not have the resources required to implement many of the CM controls required by NIST. Since OPM has defined a CM program, Recommendation 18 comes from the metrics to establish a structure for ongoing process improvement to help the CM program operate as effectively as possible, irrespective of resource constraints. This recommendation could be addressed prior to or concurrently with Recommendation 17. We feel that this recommendation is both timely and appropriate because it seeks to implement a FISMA-prescribed process designed to improve the CM programs efficiency. We continue to recommend that OPM document the lessons learned from its configuration management activities on an ongoing basis and update its configuration management plan as appropriate.

Metric 16 – Implementation of Policies and Procedures

FY 2019 Maturity Level: 2 – Defined. OPM has defined organization-wide CM policies and procedures, but has not consistently implemented many of the controls outlined in these policies, such as:

- Establishing and maintaining baseline configurations and inventories of information systems;

- Routinely verifying that information systems are actually configured in accordance with baseline configurations; and

- Conducting routine vulnerability scans on all information systems and remediating any vulnerabilities identified from the scan results in a timely manner.

Further details regarding these weaknesses are discussed with Metrics 17, 18, and 19, below.

Metric 17 – Baseline Configurations

FY 2019 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 or configuration items within those 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 cannot currently run baseline configuration checks to verify that information systems are compliant with pre-established baseline configurations, as they have yet to be developed.

NIST SP 800-53, Revision 4, requires 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 19 (Rolled forward from FY 2017)

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

OPM Response:

"We concur with the recommendation. We are working toward development and implementation of the standard configuration settings for all OPM information systems. We will work towards implementing the standard configuration settings for new deployments of operating platforms through enhancements to its [ECM] process in the upcoming fiscal year."

Recommendation 20 (Rolled forward from FY 2017)

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.

OPM Response:

"We concur with the recommendation. We plan to expand the OPM ECM program to include baseline configuration compliance. We are also considering the feasibility of expanding our change management process to a configuration management process. We will continue to conduct routine compliance scans while adding OPM information systems as is appropriate."

Metric 18 – Security Configuration Settings

FY 2019 Maturity Level: 1 – Ad-Hoc. DHS makes the distinction between implementing baseline configurations (Metric 17, above) and implementing standard security configuration settings (Metric 18). While OPM does utilize the Defense Information Systems Agency Security Technical Implementation Guides, OPM has not implemented the process for exceptions, which means OPM did not customize the configuration settings for its systems and environment. As a result, testing against the Guides is not effective since OPM did not document the allowed deviations.

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. As noted above, without formally documented and approved configuration settings, OPM cannot consistently run automated scans to verify that information systems maintain compliance with the pre-established configuration settings. Routine compliance scanning ensures that the configuration is not changed after initial implementation of security settings, which is a vital step to maintain a secure environment.

Recommendation 21 (Rolled forward from FY 2014)

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

OPM Response:

"We concur with the recommendation. We developed the standard security configuration settings for all OPM operating platforms. We will work towards implementing the standard security configuration settings for new deployments of operating platforms through enhancements to its Enterprise Configuration Management process in the upcoming fiscal year."

Recommendation 22 (Rolled forward from FY 2017)

We recommend that the OCIO conduct routine compliance scans against [the standard security configuration settings] for all servers and databases in use by OPM.

Note: This recommendation cannot be addressed until Recommendation 20 above has been completed.

OPM Response:

"We concur with the recommendation. We will conduct routine compliance scans against the standard security configuration settings as part of our Enterprise Configuration Management process updates."

Recommendation 23 (Rolled forward from FY 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:

"We concur with the recommendation. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. The OCIO completed an ISSO service requirement gap analysis which was a critical step to obtain the appropriate resources. [The] OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs will be able to better document the approval of deviations."

Metric 19 – Flaw Remediation and Patch Management

FY 2019 Maturity Level: 2 – Defined. OPM routinely performs automated vulnerability and patch compliance scans on its systems. While OPM's vulnerability scanning program has continued to improve over the last year, our audit test work indicated that several problems still exist.

Specifically, we performed a vulnerability scan on approximately 200 servers from OPM's server inventory. There are a significant number of findings, dating back to 2016, which OPM should have remediated. Therefore, OPM is either not installing the patches in a timely manner or failing to document necessary exceptions to the patching policy.

OPM does not have a process to ensure that new devices are included in vulnerability scanning.

In addition, we determined that OPM is not routinely scanning every device on its network, nor is there a formal process in place to ensure that all new devices on the agency's network are included in the scanning process.

The agency could also improve its remediation process. OPM currently distributes system specific, vulnerability scan results to the various system owners so that they can remediate the weaknesses identified in the scans. Formal POA&M entries are created for weaknesses that require significant time to remediate. However, OPM does not have a process to record or track the remediation status for other routine security weaknesses identified during vulnerability scans.

NIST SP 800-53, Revision 4, requires 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 . . . ."

NIST SP 800-53, Revision 4, states that "Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators . . . ." Furthermore, NIST SP 800-53, Revision 4, states that the organization should implement privileged access authorization for vulnerability scanning activities. "Privileged access authorization to selected system components facilitates more thorough vulnerability scanning and also protects the sensitive nature of such scanning."

Failure to formalize the process to scan the environment and track known vulnerabilities significantly increases the risk that systems will indefinitely remain susceptible to attack.

Recommendation 24 (Rolled forward from FY 2014)

We recommend that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.

OPM Response:

"We concur with this recommendation. The process and requirements include the immediate inclusion of the device into OPM's routine scanning repository. OPM controls all devices that are connecting to the network. OPM will produce evidence to support closure of this recommendation in FY 2020."

Recommendation 25 (Rolled forward from FY 2014)

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.

OPM Response:

"We concur with the recommendation. The OCIO completed an ISSO funding requirement gap analysis which was a critical component of [the] OCIO['s] efforts to obtain the appropriate funding. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. [The] OCIO continues to take steps to hire the adequate number of ISSOs through the ISSO funding model. We believe the ISSOs will be able to effectively track vulnerability scans in POA&Ms."

Recommendation 26 (Rolled forward from FY 2014)

We recommend that the OCIO implement a process to apply operating system and third party vendor patches in a timely manner.

OPM Response:

"We concur with the recommendation. [The] OCIO has a process for patch management to help ensure timely deployment of patches. We have seen significant improvements in patch management timeliness as well as an increase in our ability to deploy patches over the past year. However, going forward, [the] OCIO will work to improve consistency in the area of patch management."

Recommendation 27 (Rolled forward from FY 2018)

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

OPM Response:

"We concur with this recommendation. Projects involving changes to the environment that include new server installations should not be considered complete until this action is completed. We have identified security actions that should be completed based on types of changes that are made in the environment which will be integrated into the change control process. OPM will evaluate further implementation plans in FY 2020."

Metric 20 – Trusted Internet Connection Program

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented controls to monitor and manage its approved trusted internet connections. This has allowed OPM to meet OMB requirements related to the trusted internet connections initiative. Any improvements that need to be made to the agency's current trusted internet connections controls are documented within the organization's POA&M.

Metric 21 – Configuration Change Control Management

FY 2019 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 required documentation needed 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.

Metric 22 – Configuration Management Other Information

There are no additional comments regarding configuration management.

D. IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

The Federal Identity, Credential, and Access Management (FICAM) program is a government-wide effort to help Federal agencies provision access to systems and facilities for the right person, at the right time, for the right reason. While OPM still has room for maturity in this area, the agency has successfully implemented 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 "3 – Consistently Implemented."**

Metric 23 – ICAM Roles, Responsibilities, and Resources

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM has documented policies and procedures that outline its agency-wide system account and identity management program roles and responsibilities. This includes procedures for creating user accounts with the appropriate level of access and procedures for removing access for terminated employees.

However, OPM does not consider ICAM to be a distinct program. In FY 2017, it was determined that OPM did not have a process in place to ensure that it provides adequate resources (people, processes, and technology) to stakeholders to fully implement ICAM controls. The agency took no corrective actions in FY 2018 or FY 2019. As OMB Memorandum M-19-17 requires agencies to develop an ICAM program, OPM now acknowledges the need for a formal program.

FICAM Roadmap Implementation Guidance states, "As part of the [Logical Access Control Systems] modernization planning effort, agencies should evaluate their logical access policies and identify potential gaps where revisions, updates, and new policies and/or standards are needed to drive the process and underlying technology changes . . . ." The guidance also states, "an agency should assess its organizational structure, identity stores/repositories, access control processes, and IT resources when planning new or modifying existing [Logical Access Control Systems] investments."

Failure to identify the necessary resources required to maintain and progress OPM's ICAM program increases the risk of controls not being manageable or effective.

Recommendation 28 (Rolled forward from FY 2017)

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.

OPM Response:

"We concur with this recommendation. While OPM did not previously consider ICAM to be a distinct program, in order to further improve in this metric and meet the intent of OMB Memorandum M-19-17, OPM will work to establish a distinct ICAM program."

Metric 24 – ICAM Strategy

FY 2019 Maturity Level: 1 – Ad Hoc. In FY 2017, it was determined OPM has not developed and implemented an ICAM strategy containing milestones for how the agency plans to align with Federal ICAM initiatives. As noted above, OPM had not considered ICAM to be a distinct program and thus there were no corrective actions in FY 2018 or FY 2019.

OPM has not developed and implemented an ICAM strategy.

OPM has now acknowledged, with the new OMB Memorandum M-19-17, that it must develop a distinct ICAM program and indicated it will begin this effort in FY 2020.

FICAM Roadmap Implementation Guidance states "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 ICAM segment architecture has been adopted as an approved segment within the [Federal Enterprise Architecture], which agencies are required to implement."

Failure to formalize an ICAM strategy that includes a review of current practices, identification of gaps, and a transition plan can prevent OPM from ensuring the success of its ICAM initiatives.

Although OPM has successfully implemented many ICAM-related controls, the development of a comprehensive ICAM strategy will help to ensure the success of the agency's ICAM program.

Recommendation 29 (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:

"We concur with this recommendation. While the agency did not previously consider ICAM to be a distinct program, OPM will work to meet the intent of OMB Memorandum M-19-17. We plan to conduct a gap analysis in FY 2020."

Metric 25 – Implementation of ICAM Program

FY 2019 Maturity Level: 2 – Defined. OPM has defined many of the required elements of a comprehensive ICAM program (Metrics 26 – 31, below). However, OPM has not implemented Personal Identity Verification (PIV) authentication at the application level (Metric 28, below), and does not adequately manage contractor accounts (Metric 32, below).

As explained above OPM has not recognized ICAM as a distinct program and does not capture or share lessons learned on the effectiveness of its ICAM controls.

The FICAM Roadmap Implementation Guide states that "Working groups are also used as a forum for sharing implementation lessons learned across bureaus/components or individual programs in order to reduce overall ICAM program risk and increase speed and efficiency in implementation."

Failure to consistently capture and share lessons learned on the efficacy of an ICAM program increases the risk of resources used in an ineffective manner.

Recommendation 30 (Rolled forward from FY 2017)

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.

OPM Response:

"We concur with this recommendation. While OPM did not previously consider ICAM to be a distinct program, OPM will work to meet the intent of OMB Memorandum M-19-17 and conduct the analysis referenced in Recommendation 29. After Recommendation 29 analysis

has been completed, OPM can then address this recommendation to capture and share lessons learned."

Metric 26 – Personnel Risk

FY 2019 Maturity Level: 4 – Managed and Measurable. OPM has defined and implemented processes for assigning personnel risk designations and performing appropriate screenings prior to granting access to its systems. OPM has also implemented an automated process to centrally document, track, and share risk designations and screening information with necessary parties. Additionally, OPM re-screens individuals when they change positions or the risk designation of their current position is changed.

Metric 27 – Access Agreements

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented processes for developing, documenting and maintaining access agreements for all users of the network. Users must sign the access agreements prior to gaining any network or system access. The agency also utilizes additional agreements for privileged users or those with access to sensitive information, as appropriate.

Metric 28 – Multi-factor Authentication with PIV

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM has enforced multi-factor authentication for non-privileged users for facility, network, and remote access using PIV cards. OPM continues to expand its PIV implementation incrementally. However, it has not configured multi-factor authentication for all major systems.

OMB Memorandum M-11-11 required all Federal information systems to use PIV credentials for multi-factor authentication by FY 2012. Since that time, OMB Memorandum M-19-17 was issued, superseding the prior memorandum, but it continues to require that all new systems under development must be PIV compliant prior to being made operational.

Failure to enforce PIV authentication for major information systems increases the risk of an attacker gaining unauthorized access to sensitive data.

Recommendation 31 (Rolled forward from 2012)

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.

Note: OMB updated the guidance referenced in this recommendation with the issuance of OMB M-19-17. As such, OPM should ensure its PIV compliance efforts align to the new guidance. We have not adjusted the language of the recommendation and continue to roll forward the recommendation as the new guidance still requires OPM to update its major information systems to require multi-factor authentication using PIV credentials.

OPM Response:

"We concur with the recommendation. OPM will work to meet the intent of OMB Memorandum M-19-17 (which has superseded M-11-11) and revisit plans on how to address this recommendation."

Metric 29 – Strong Authentication Mechanisms for Privileged Users

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM has enforced multi-factor authentication for privileged user access to the OPM network and its back-end servers. There are no exceptions made for privileged user access.

Metric 30 – Management of Privileged User Accounts

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM has developed and implemented processes for provisioning, managing, and reviewing privileged user accounts. The OCIO restricts privileged user account functions and restricts session durations. Additionally, the OCIO records, logs, and periodically reviews account sessions.

Metric 31 – Remote Access Connections

FY 2019 Maturity Level: 4 – Managed and Measurable. OPM has implemented a variety of controls for remote access connections such as the use of cryptographic modules, system time outs, and monitoring remote access sessions. The agency ensures that remote access users' activities are logged and periodically reviewed. In addition, OPM verifies that user devices have been appropriately configured prior to allowing remote access, and restricts the ability of individuals to transfer data accessed remotely to non-authorized devices.

Metric 32 – ICAM Other Information – Contractor Access Management

OPM has defined and implemented processes for managing Federal employees' physical and logical access to sensitive resources. However, OPM does not centrally manage terminating contractor access. Furthermore, OPM does not maintain a complete list of all contractors who

have access to OPM's network, so there is no way for the OCIO to audit the termination process to ensure timely removal of contractor accounts.

OPM is in the preliminary phases of deploying a tool that will maintain all current user records and enable user account auditing, to include contractor accounts. However, the tool is being configured and is not completely operational.

OPM does not maintain a complete list of all contractors who have access to OPM's network.

FISCAM states that "Contractors that provide systems and services or other users with privileged access to agency/entity systems, applications, and data can introduce risks to their information and systems; for example, contractors often provide unsupervised remote maintenance and monitoring of agency/entity systems." It also states that "Terminated employees who continue to have access to critical or sensitive resources pose a major threat . . . ."

Failure to maintain an accurate and up-to-date list of contractors with access to OPM systems increases the risk of inappropriate access to critical or sensitive resources.

Recommendation 32 (Rolled forward from 2016)

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.

OPM Response:

"We concur with the recommendation. The OCIO has incorporated all contractors into the centralized tool and master user record however processes have not yet been established for routine user account audit or review. OPM relies on support from the [DHS CDM] program to support the implementation of these requirements. OPM continues to be at the forefront of working with DHS on the CDM program and will maintain this partnership as CDM evolves."

E. 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 "1 – Ad-hoc."**

Metric 33 – Data Protection and Privacy Policies and Procedures

FY 2019 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, OPM has not updated this handbook since 2011, and it does not contain the personally identifiable information (PII) protection plans, policies, and procedures necessary for a mature privacy program. OPM established the Chief Privacy Officer position and the Office of Privacy and Information Management (OPIM) in 2016 and 2019, respectively. Despite this substantial stride, OPM has not clearly defined the additional roles and responsibilities to support the program. The resource constraints within the OPIM are evident by the fact that the owners of 14 of OPM's major information systems have not completed a current privacy assessment. Additionally, several draft privacy policies are still going through OPM's Office of General Council policy review process.

NIST SP 800-53, Revision 4, requires that the organization "Develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures . . . ."

Failure to have a strong privacy program in place increases the agency's risk for data loss and mishandling of sensitive information.

Recommendation 33 (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:

"We do not concur with this recommendation. We disagree that no roles and responsibilities for privacy are currently defined at OPM. The agency has made significant progress toward fully defining the roles and responsibilities for OPM's privacy program to date. The [OPIM] was established in February . . . 2019, in order to elevate and co-locate certain important and complementary subject matter areas and, in so doing, call attention to their significance in the day-to-day business operations of OPM and to ensure they were properly resourced. This included realigning the former Information Management and Freedom of Information Act . . . groups from the [OCIO] into [the] OPIM and realigning the Chief Privacy Officer/Senior Agency Official for Privacy [(SAOP)] from within the Office of the Director to lead the new organization. [The] OPIM's key areas of responsibility are: Privacy; Freedom of Information Act; Records Management; Section 508 Accessibility; Forms Management/Paperwork Reduction Act; and Controlled Unclassified Information . . . .

Additionally, OPM elevated the Chief Privacy Officer/[SAOP] to a senior-level position reporting directly to the Director of OPM in 2016. That position, based on the position description and the requirements set forth in guidance from the [OMB] (Memorandum 16-24) and Executive Order 13719. The SAOP has responsibility for privacy policy and compliance at OPM, and has the necessary authority at the agency to lead and direct OPM's privacy program to carry out the privacy-related functions described in law and OMB policies."

OIG Comment:

We acknowledge that OPM has some defined roles within its privacy program. However, the program is still in its infancy and this recommendation, along with Recommendation 34, provide OPM the ability to show incremental progress as OPM develops its new office. Fully defining roles and responsibilities, as well as developing policies, are both necessary as OPM builds its privacy program. OPM must define its agency-wide privacy program, not just a single position of responsibility. We understand that the changes made this year can greatly increase the effectiveness of the privacy program. However, without a fully defined structure and complete identification of necessary positions, it will be very difficult to ensure that the OPIM has sufficient resources to fulfill its assigned responsibilities. We continue to recommend that OPM define the roles and responsibilities for its privacy program.

Recommendation 34 (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:

"We partially concur with this recommendation. We agree that a more focused articulation of privacy policies and procedures that are separate from and/or integrated with information security policy and procedures, is appropriate. The formation of [the] OPIM is the initial step towards that end. We disagree that there are not currently in place plans, policies, and procedures for the protection of PII. The Information Security and Privacy Policy Handbook includes appropriate privacy provisions, as do the current [Privacy Impact Assessments] and [Privacy Act System of Records Notice] guides. In addition, the Chief Privacy Officer implemented a robust template for [the] Privacy Impact Assessments . . . that has been in use since 2016, as well as a template for Privacy Threshold Analyses . . . . The [Privacy Threshold Analyses] template has been implemented both to determine the need for a [Privacy Impact Assessments] or a Privacy Act system of records notice and to track appropriate privacy controls as articulated in NIST [SP] 800-53, Appendix J. In addition to those OPM-specific policies and procedures, the agency continues to rely on overarching privacy guidance issued

by the OMB and NIST. The [Privacy Impact Assessments] template follows the prescribed questions required by the eGovernment Act of 2002. The [Privacy Act System of Records Notice] template follows the guidance from OMB Circular A-108. Other documents and templates are being developed in the OPIM . . . to better enable information management and privacy-related education."

OIG Comment:

We acknowledge that the creation of the OPIM is a positive step for OPM's privacy program. However, there are still significant steps that the program needs to be fully functional. OPM's current privacy program is based on policy written in 2011. The policy does not include the current privacy controls required by NIST in SP 800-53 Appendix J published in 2013, or Circular A-130 published in 2016. We acknowledge that OPM updated some procedures and templates. Nevertheless, we continue to identify issues surrounding privacy controls at OPM including the implementation of the updated procedures. As noted above, OPM authorized 14 major systems that did not have a current privacy assessment. The agency must implement effective plans, policies, and procedures to constitute a comprehensive privacy program as required by both NIST and OMB. As such we continue to recommend that OPM develop its privacy program by creating the necessary plans, policies, and procedures for the protection of PII.

Metric 34 – Data Protection and Privacy Controls

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM has implemented both policies and technical controls to protect data in its IT environment. These include controls to protect data at rest, data in transit, and to limit the transfer of information via removable media.

Metric 35 – Data Exfiltration Prevention

FY 2019 Maturity Level: 4 – Managed and Measurable. OPM has defined policies to limit data exfiltration from its IT environment and for implementing enhanced network defenses. OPM has implemented controls to monitor inbound and outbound network traffic, as well as ensure all traffic passes through a web content filter. In addition, the agency has implemented a process to measure the effectiveness of the controls on an ongoing basis.

Metric 36 – Data Breach Response Plan

FY 2019 Maturity Level: 2 – Defined. OPM has defined and communicated its Data Breach Response Plan and established a data breach response team. However, OPM does not currently

conduct routine exercises to test the Data Breach Response Plan. The plan itself identifies the requirements for quarterly reviews and annual testing.

NIST SP 800-122 requires 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 increases the organization's risk of major data loss in the event of a security incident.

Recommendation 35 (Rolled forward from 2018)

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

OPM Response:

"We concur with this recommendation. We agree that an annual exercise to review the Breach Response Plan can help clarify and refine roles and responsibilities in the event of a breach and help to more clearly articulate the appropriate risk analysis and mitigation steps that should be taken, as provided by the Breach Response Plan and OMB Memorandum 17-12.

Though no formal test of the Data Breach Response Plan has occurred, there have been instances where the OPM Security Operations Center . . . routinely informs appropriate OPM personnel when an incident has occurred and steps were taken to address and mitigate any potential harm as appropriate. [The] OPIM staff routinely reviews PII incident reports/breaches received from the [Security Operations Center] and advises the Chief Privacy Office as necessary. The Chief Privacy Officer is a part of the senior members of the OPM staff that routinely meets and interacts with other key members of the workforce, which allows for consistent communication regarding the protection of sensitive identifiable information to occur."

Metric 37 – Privacy Awareness Training

FY 2019 Maturity Level: 1 – Ad hoc. OPM has defined and communicated its privacy awareness training program throughout the agency. OPM tailors training to the agency's risk environment, ensures that all employees receive basic privacy awareness training on an annual basis, and requires all users to accept a rules of behavior notice prior to logging onto the network. However, individuals with responsibilities for PII or activities involving PII do not receive elevated role-based privacy training. OPM's current policy states that system owners are

responsible for providing role-based training and that users must "complete role-based security or privacy training if assigned a significant security or privacy role."

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 . . . ." In addition, OMB Memorandum 17-12 highlights the need for specialized training for individuals working with High Value Assets.

OPM does not require role-based privacy training.

Furthermore, NIST SP 800-53, Revision 4, requires that the organization "Administers basic privacy training . . . and targeted, role-based privacy training for personnel having responsibility for [PII] or for activities that involve PII [at least annually] . . . ."

Failure to provide individuals specific training according to their role in identifying, processing, and managing PII increases the organization's risk of mishandled data, which could result in a data loss incident.

Recommendation 36 (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:

"We partially concur with this recommendation. We agree that appropriate annual privacy training should be provided. This is done formally through the annual security and privacy awareness training that all individuals at OPM are required to complete. We also agree that it would be beneficial to evaluate more formally whether there are individuals who, given their job responsibilities and exposure to PII, should receive any additional annual training.

We disagree with the underlying assumption that individuals who regularly handle PII will always require specialized formal annual training. In many instances the annual awareness training, followed by tailored discussions with various offices, can be just as effective. To date, the Chief Privacy Officer has provided presentations on privacy and engaged in group discussions with various offices in an effort to further provide appropriate privacy awareness and compliance."

OIG Comment:

There is no assumption that all individuals that regularly handle PII will require specialized training. As noted above, both OMB and NIST require that there be role-based training requirements for individuals with heightened responsibility for PII. Our recommendation is that OPM identify those individuals and roles with heightened responsibilities, not necessarily every user or individual with access to PII, and provide relevant training to their specific job function as a steward of PII. There are many roles that could be identified (e.g., ISSOs, system owners, data owners, program managers, executives, etc.) which could necessitate additional training on how to implement the required privacy controls and processes to protect PII at OPM. Additionally, this would likely include individuals working in OPM's OPIM to ensure that those designing the agency's privacy program have current and appropriate understanding of privacy requirements and best practices. We continue to recommend that OPM identify individuals with heightened responsibility for PII and provide relevant role-based training to these individuals at least annually.

Metric 38 – Other Information Data Protection and Privacy

There are no additional comments regarding data protection and privacy.

F. 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 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 "4 – Managed and Measurable."**

Metric 39 – Security Training Policies and Procedures

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM has developed and established an agency-wide IT security awareness training program. The agency has defined stakeholder roles and responsibilities and communicated them across the organization. OPM is continuing to improve its security training program by developing a process to consistently collect, monitor, and analyze qualitative and quantitative performance measures of the security awareness training activities.

Metric 40 – Assessment of Workforce

FY 2019 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 made progress in this area, a gap analysis, to determine any weaknesses and specialized training needs, must be performed.

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."

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 37 (Rolled forward from 2017)

We recommend that OPM develop and conduct an 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 skills gaps and training needs has not been performed.

OPM Response:

"We partially concur with this recommendation. [The] OCIO has adhered to the guidance received and feels it has met the intent of the Federal Cybersecurity Workforce Assessment Act of 2015. OPM will continue to work towards the goals necessary to [fulfill] specialized training needs."

OIG Comment:

We acknowledge that OPM has performed the required assessment. However, OPM has not used the assessment to identify the gaps or needs for specialized training or skills development. Using the assessment results to improve OPM's workforce and resources is the crucial next step for the agency. We continue to recommend that OPM utilize the assessment of its workforce's knowledge, skills, and abilities to identify any skill gaps and specialized training needs.

Metric 41 – Security Awareness Strategy

FY 2019 Maturity Level: 2 – Defined. As of November 2018, OPM had developed a strategic plan for the cybersecurity policy team, which included security awareness training tailored to its mission and risk environment. Additionally, OPM assessed its workforce's current knowledge, skills, and abilities (Metric 40, above). However, OPM has not performed the gap analysis to identify the training needs. The analysis will allow OPM to improve its plan and efficiently address the identified gaps.

Metric 42 – Specialized Security Training Policies

FY 2019 Maturity Level: 4 – Managed and Measureable. OPM has established policies and procedures that require agency employees to take security awareness and specialized security training. OPM is working to improve its security training program by implementing a process to measure the effectiveness of specialized training.

Metric 43 – Tracking IT Security Training

FY 2019 Maturity Level: 4 – Managed and Measureable. 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, viruses and malicious code, 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 in order to measure the effectiveness of the exercises. OPM also conducts associated follow-up exercises and the results are used to update the IT security training program. More than 92 percent of OPM's employees and 98 percent of contractors completed the security awareness training course in FY 2019.

Metric 44 – Tracking Specialized IT Security Training

FY 2019 Maturity Level: 4 – Managed and Measureable. 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 specialized training taken by employees with security responsibility. The position and corresponding level of security responsibility define these individuals' training requirements (i.e., number of training hours). The supervising program offices manage the specific training curriculums.

Metric 45 – Security Training Other Information

There are no additional comments regarding the security training program.

G. INFORMATION SECURITY CONTINUOUS MONITORING

Information Security Continuous Monitoring (ISCM) controls involve the ongoing assessment of control effectiveness in support of the agency's efforts to manage information security vulnerabilities and threats. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Information Security Continuous Monitoring domain is "2 – Defined."**

Metric 46 – ISCM Strategy

FY 2019 Maturity Level: 2 – Defined. OPM has developed an ISCM strategy that addresses the monitoring of security controls at the organization, business unit, and individual information system level. At the organization and business unit level, the ISCM strategy defines how the agency's activities support risk management in accordance with organizational risk tolerance. At the information system level, the ISCM strategy establishes processes for monitoring security controls for effectiveness and reporting any findings.

However, in practice, OPM is not consistently implementing several of the objectives outlined in its ISCM strategy, including:

- "Security controls must be assessed to ensure continued effectiveness of their implementation and operation[;]"
- "Identified threats and vulnerabilities must be reported timely to support risk management decisions[;]" and
- "Feedback must be collected frequently and incorporated into a system of continually improving processes."

At this stage in the development of its ISCM program, OPM has not consistently implemented the ISCM strategy and has not met its objective of providing stakeholders with sufficient information to evaluate risk. The ISSOs are responsible for continually assessing security controls for each major system. The ISSOs should be competent, knowledgeable, and capable of properly managing the overall program. OPM's failure to consistently implement the ISCM strategy is a direct result of its inability to fully staff information security positions (Metric 48,

below). As a result, only 8 of OPM's 47 systems were subject to adequate security controls testing and monitoring in FY 2019 (Metric 49, below).

Metric 47 – ISCM Policies and Procedures

FY 2019 Maturity Level: 2 – Defined. OPM has developed ISCM policies and procedures tailored to its environment including specific requirements and deliverables. However, regular testing is not conducted for many of OPM's major information systems. Only 8 of its 47 major systems were adequately tested (Metric 49, below). Additionally, when testing does occur, OPM does not capture lessons learned to make improvements to ISCM policies and procedures. OPM needs to perform regular ISCM testing before it can implement an improvement process using lessons learned.

Metric 48 – ISCM Roles, Responsibilities, and Resources

FY 2019 Maturity Level: 2 – Defined. OPM has defined the structure, roles, and responsibilities of its ISCM teams and stakeholders. OPM has also conducted an analysis to identify resource gaps in the ISCM program. The analysis identified and quantified the resource gap and confirms that the agency still does not have adequate resources to implement the activities effectively required by its ISCM strategy and policies.

NIST SP 800-137 states that the "ISCM helps to provide situational awareness of the security status of the organization's systems based on information collected from resources (e.g., people, processes, technology, [and] environment) and the capabilities in place to react as the situation changes."

Failure to apply the resources needed to perform ISCM activities results in limited ability to protect sensitive information and ensure that security controls are operating effectively.

Recommendation 38 (Rolled Forward from 2017)

We recommend that OPM conduct an analysis to identify any resource gaps within its current ISCM program. OPM should use the results of this gap analysis to ensure stakeholders have adequate resources to implement ISCM activities effectively based on OPM's policies and procedures.

OPM Response:

"We concur with the recommendation. The OPM [Chief Information Officer] completed an ISSO funding requirement gap analysis which was a critical component of [the] OCIO['s]

efforts to obtain the appropriate funding. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. [The] OCIO continues to take steps to hire the adequate number of ISSOs through the ISSO funding model."

Metric 49 – Ongoing Security Assessments

FY 2019 Maturity Level: 2 – Defined. Historically, OPM has struggled in two areas to implement critical FISMA controls over security assessments. The first area concerns OPM's ability to implement the Authorization process for allowing systems into its environment. The second area concerns the regular testing of security controls. OPM has defined its processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls for individual systems. Additionally, this year OPM has demonstrated an improved Authorization process; however, regular testing of security controls still represents an area of weakness for the agency.

1) Security Assessment and Authorization

OPM has documented security categorizations and risk assessments for all 47 major systems. In addition, OPM had a current Authorization for all 47 systems at one point in FY 2019.

We did observe that 6 of the 47 Authorizations provided were signed by an agency official who is no longer with OPM, a fact that necessitates re-authorization by the new authorizing official. OPM policies and procedures do not currently address when an agency official in the Authorization process changes roles or is no longer with the agency.

Six of the Authorizations were signed by an agency official who is no longer with OPM.

This was first identified in the Data Center Optimization Initiative Audit, Report No. 4A-CI-00-19-008, where we recommended that "OPM update its Authorization policies and procedures to include requirements for reauthorizing systems in the event of a change in authorizing official." This recommendation remains open.

The NIST SP 800-37, Revision 2, requires that "When there is a change in authorizing officials, the new authorizing official reviews the current authorization decision document, authorization package, any updated documents from ongoing monitoring activities, or a report from automated security/privacy management and reporting tools. If the new authorizing official finds the current risk to be acceptable, the official signs a new or updated authorization decision document, formally transferring responsibility and accountability for the system or the common controls [and] . . . explicitly [accepting] the risk . . . ."

Failure to update a system's documentation and Authorization when an Authorizing Official leaves increases the risk that the system will operate without proper risk management oversight and accountability.

Recommendation 39 (Rolled forward from 2014)

We recommend that all active systems in OPM's inventory have a complete and current Authorization.

OPM Response:

"We partially concur with your recommendation. The OIG found that while OPM had current authorizations for all of its major systems at [one] point in FY [2019], six of these authorizations were signed by an agency official no longer with OPM as of issuance of the OIG's draft report. We understand and agree with the need to have a new Authorizing Official re-evaluate authorizations in such circumstances. However, the current NIST guidance in this area permits a range of actions that can be taken including, for example, the signing of a new formal authorization document, reauthorization, or ongoing authorization. With the flexibility afforded agencies in determining how the guidelines will apply, OPM will review and take appropriate action for authorization packages consistent with updated policies."

OIG Comment:

The requirement that all systems be authorized to operate comes from both NIST and OMB guidance. Our recommendation follows that guidance. We agree that OPM has multiple paths that can be followed when an official leaves the agency and that the agency has discretion in creating policy that governs how that process will work. With proper inputs, each case described in OPM's response should result in a current authorization decision and meet the requirements of NIST, OMB, and the intent of the recommendation.

Recommendation 40 (Rolled forward from 2014)

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.

OPM Response:

"We partially concur with the recommendation. We have taken, and will continue to take, [the] OIG's recommendation under advisement and agree that system owners provide support to the business processes of the agency. Apart from changes to performance standards, OPM will continue to identify appropriate ways to work with system owners to help ensure FISMA compliance. For instance, recently issued cybersecurity policies set forth expectations and requirements for system owners, consistent with NIST 800 Series guidance."

OIG Comment:

System owners are responsible for ensuring that the proper controls and approvals are in place for their information systems and aligning their performance standards to this assigned responsibility should help to ensure they achieve this critical objective of authorizing systems. This recommendation has been open for more than five years and system Authorizations are still a hurdle for the agency. Accountability is a critical step towards achieving objectives and thus far the agency's alternate methods, of working with the system owners to help ensure FISMA compliance, have not been successful. We continue to recommend that the agency modify the performance standards of all OPM system owners 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.

2) Controls Testing

We continue to find that many systems are not following the security control testing schedule that the OCIO mandated for all systems. OPM's policy requires that evidence of security control testing be provided to the OCIO on a quarterly basis.

For the first three quarters of FY 2019, OPM provided evidence of security control testing for 28 of OPM's 47 major systems. Of those, only eight systems were subject to security controls testing that complied with OPM's ISCM submission schedule for all three quarters.

While resource limitations certainly impact OPM's cybersecurity program, we believe that lack of effective management is a contributing factor. Monitoring efforts, following up on incomplete results, evaluating the quality of work products, and reporting to senior leadership and other stakeholders are basic elements of a properly managed program. OPM has not been able to test the security controls of its systems adequately for at least 10 years.

FISMA requires agencies to "conduct assessments of security controls at a frequency appropriate to risk, but no less than annually."

Failure to complete a comprehensive security controls test for all information systems and use the results to establish a risk baseline for the agency prevents OPM from moving forward in implementing its ISCM strategy. Furthermore, OPM is at risk of an attack that exploits vulnerabilities that could have been identified had security controls testing been completed.

Recommendation 41 (Rolled forward from 2008)

We recommend that OPM ensure that an annual test of security controls has been completed for all systems.

OPM Response:

"We concur with the recommendation. The OCIO completed an ISSO funding requirement gap analysis which was a critical component of [the] OCIO ['s] efforts to obtain the appropriate funding. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. [The] OCIO continues to take steps to hire the adequate number of ISSOs through the ISSO funding model."

Metric 50 – Measuring ISCM Program Effectiveness

FY 2019 Maturity Level: 2 – Defined. OPM has identified and defined the performance measures and requirements to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk.

However, OPM has not defined the format of reports measuring its ISCM program effectiveness. In addition, OPM has failed to complete the first step necessary to assess the effectiveness of its ISCM program – to collect the necessary baseline data by actually assessing the security controls of its systems. To reach the next level in the ISCM maturity model OPM needs to consistently capture the performance measures needed to evaluate the effectiveness of the ISCM program.

NIST SP 800-137 states that an organization must "Analyze the data collected and Report findings, determining the appropriate response." Furthermore, "Organizations [must] develop procedures for collecting and reporting assessment and monitoring results, including results that are derived via manual methods, and for managing and collecting information from POA&Ms to be used for frequency determination, status reporting, and monitoring strategy revision."

Failure to define reporting formats and consistently capture performance measures can impede OPM's ability to evaluate the effectiveness of the ISCM program, and increase the risk that OPM is not implementing security controls according to agency policy.

Recommendation 42

We recommend that OPM define a format for the reports used to communicate the effectiveness of its ISCM program.

OPM Response:

"We do not concur with this recommendation. As noted in the report, OPM identified and defined performance measures. We are collecting and analyzing these performance measures and using our centralized repository tool and associated reporting format. This report format was provided to the OIG upon review of the draft recommendations."

OIG Comment:

In response to the Notice of Finding and Recommendation, we received a report structure for OPM's POA&Ms not specific to ISCM. No additional documentation was provided with OPM's response to the draft audit report. During fieldwork discussions, OPM indicated that the processes for collecting and evaluating ISCM performance metrics was still being designed and implemented. No evidence was discussed or provided during the audit that indicates OPM has a documented reporting format to monitor the effectiveness of its ISCM program. We continue to recommend that OPM define a format for the reports used to communicate the effectiveness of its ISCM program. Please provide the appropriate and adequate evidence to OPM's Internal Oversight and Compliance office to support closure of this recommendation.

Recommendation 43 (Rolled forward from 2017)

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 41.

OPM Response:

"We do not concur with this finding. As noted in the report, OPM identified and defined performance measures. We are collecting and analyzing the performance measures based on consistently obtained security assessment control report. Additionally, the agency uses our centralized repository tool reports for evaluation purposes."

OIG Comment:

OPM's ISCM program has not demonstrated an ability to consistently collect security assessment control information. As noted above, during 2019, only 28 of 47 systems were subjected to any ISCM assessments, and only 8 systems were subject to ISCM assessments in all of the three quarters we reviewed. OPM must consistently acquire sufficient assessment results before it is capable of evaluating the performances measures and the effectiveness of its ISCM program.

Metric 51 – ISCM Other Information

There are no additional comments regarding OPM's ISCM program.

H. INCIDENT RESPONSE

Incident response is an organized approach for reacting to a cyber-attack 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, and we have no audit recommendations in this area.** 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."**

OPM's overall maturity level for the Incident Response domain is "4 – Managed and Measurable."

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

FY 2019 Maturity Level: 4 – Managed and Measureable. OPM has defined, communicated, and consistently implemented its incident response policies, procedures, plans, and strategies. OPM is consistently capturing and sharing lessons learned on the effectiveness of its incident response program. In addition, OPM monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response program and, as appropriate, implements updates to the program.

Metric 53 – Incident Roles and Responsibilities

FY 2019 Maturity Level: 4 – Managed and Measureable. 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.

Metric 54 – Incident Detection and Analysis

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM utilizes a threat vector classification system for its incident response program, allowing the agency to quickly analyze and prioritize any incidents reported or detected. In addition, OPM has implemented several security tools to analyze precursors and indicators of security threats to help it better identify possible security incidents before they occur. OPM is in the process of developing profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can effectively detect security incidents.

Metric 55 – Incident Handling

FY 2019 Maturity Level: 4 – Managed and Measureable. 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 mitigate any exploited vulnerabilities, and the recovery of systems. OPM uses metrics to measure the impact of successful incidents and is able to quickly mitigate related vulnerabilities on other systems so that they are not subject to the same exploitation.

Metric 56 – Sharing Incident Response Information

FY 2019 Maturity Level: 4 – Managed and Measureable. OPM has a documented policy that defines how it distributes incident response information with individuals with significant security responsibility. OPM also has controls in place to ensure it reports security incidents to DHS, law enforcement, the OIG, and the 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.

Metric 57 – Contractual Relationships in Support of Incident Response

FY 2019 Maturity Level: 4 – Managed and Measureable. 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.

Metric 58 – Technology to Support Incident Response

FY 2019 Maturity Level: 4 – Managed and Measureable. OPM has implemented and configured incident response tools to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures. OPM utilizes the reporting tools for monitoring and analyzing qualitative and quantitative incident response performance across the organization. OPM uses the data collected from these tools to generate monthly reports to stakeholders on the effectiveness of its incident response program.

Metric 59 – Incident Response Other Information

There are no additional comments regarding OPM's incident response capability.

I. 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 2019 Maturity Level: 2 – Defined. OPM has a policy in place that describes the roles and responsibilities of individuals that are part of the agency's contingency planning program.

The agency should perform yearly contingency plan testing and use the results to update each system's contingency plan. Evidence shows that less than a quarter of the information systems have updated contingency plans and even less have performed contingency plan testing (see Metric 61 below for additional information).

In FY 2018, it was determined that OPM does not have adequate resources to implement the agency contingency plan policy. OPM indicated the lack of consistent contingency plan testing in FY 2019 is a result of staffing shortages.

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.

OPM is at risk of not being able to restore systems in the event of a disaster.

Recommendation 44 (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 effectively implement the agency's contingency planning policy.

OPM Response:

"We concur with the recommendation. The OCIO is aware of the technology and resource gaps related to contingency plan testing. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. The OCIO completed an ISSO service requirement gap analysis which was a critical component of [the] OCIO['s] efforts to obtain the appropriate funding. [The] OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs will be able to address gaps in implementation of our contingency planning policy."

Metric 61 – Contingency Planning Policies and Procedures

FY 2019 Maturity Level: 2 – Defined. OPM has contingency planning policies and procedures in place, but does not consistently adhere to these policies. The remaining metrics in this domain outline the specific deficiencies in OPM's contingency planning program, but in summary:

Only 7 of 42 OPM's contingency plans were reviewed and updated in 2019.

- Contingency plans exist for only 42 of OPM's 47 major information systems;
- Only 7 of the 42 contingency plans were reviewed and updated in FY 2019;
- Only 5 of 42 contingency plans were tested in FY 2019; and
- Only 1 contingency plan was updated to address the test results.

It is the responsibility of the system owner for each major system to ensure that the system is subject to a contingency plan test each year and to update the plan accordingly. Failure to appropriately manage information system contingency plans in a changing environment

increases the risk that contingency plans will not meet OPM's system recovery time and business objectives should disruptive events occur. The sections below contain specific recommendations related to contingency plan management; some of these recommendations have been extremely longstanding issues at OPM.

Metric 62 – Business Impact Analysis

FY 2019 Maturity Level: 1 – Ad-Hoc. 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. Not all of OPM's major information systems have an approved BIA nor has this issue been identified in the POA&Ms.

OPM successfully performed an agency-wide BIA in March 2018 as a part of the National Continuity Program. The analysis identified the agency's Primary Mission Essential Functions and the Critical Information Technology Infrastructure that supports them. However, OPM has not incorporated the results of the BIA into the system-level contingency plans.

The OCIO needs to coordinate with the system owners and authorizing officials to ensure it communicates results and updates the system-level contingency plans to reflect the results of the BIA. While OPM updated some contingency plans after the completion of the BIA, they did not incorporate the results of the BIA. There is an apparent lack of communication when disseminating results to the system level.

NIST SP 800-53, Revision 4, requires the agency to 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."

Failure to have a current BIA in place for every major information system increases the risk that the agency would be unable to prioritize operations effectively in the event of a disruption of service or natural disaster.

Recommendation 45 (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:

"We concur with the recommendation. OPM completed an agency-wide BIA and developed a new template with instructions for incorporating the results into system-level contingency plans in May 2018. The agency expects to see the agency wide BIA results reflected in all contingency plans by the end of FY 2020."

Metric 63 – Contingency Plan Maintenance

FY 2019 Maturity Level: 2 – Defined. OPM has a policy that requires a contingency plan to be in place and routinely updated for every major information system. While OPM has made progress, it is still far from adhering to this policy.

As stated above in Metric 61, only 7 of the 47 major systems have current contingency plans that were reviewed and updated in FY 2019.

The OCIO needs to coordinate with the system owners and authorizing officials to ensure the contingency plans are in place and that an update occurs in accordance with policy. Currently, the OCIO is not sufficiently empowered to enforce the contingency planning policy.

NIST SP 800-34, Revision 1, states that "[I]t 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."

Failure to have a current contingency plan in place for every major information system increases the risk that the agency is unable to restore operations efficiently in the event of a disaster.

Recommendation 46 (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:

"We concur with the recommendation. The OCIO will coordinate with each system's Program Management Office . . . including the system owners and authorizing officials to help ensure contingency plans are in place and that the annual review and update of the plans occurs in accordance with policy."

Metric 64 – Contingency Plan Testing

FY 2019 Maturity Level: 2 – Defined. Routinely testing contingency plans is a critical step in ensuring that plans can be successfully executed in the event of a disaster. Only 5 of the 47 major information systems were subject to an adequate contingency plan test in FY 2019. Additionally, more than 60 percent of the major systems have not been tested for 2 years or longer.

The OCIO needs to coordinate with each system's owner and authorizing official to update and annually test the contingency plans in accordance with policy. The OPM Contingency Planning Policy requires system owners to "Test the contingency plan for the information system [at least annually] . . . ."

NIST SP 800-53, Revision 4, states that organizations should test "the contingency plan for the information system . . . to determine the effectiveness of the plan and readiness to execute the plan . . . ."

Failure to perform contingency plan testing for every major information system increases the risk that the agency is unable to restore operations efficiently in the event of a disaster.

Recommendation 47 (Rolled forward from 2008)

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

OPM Response:

"We concur with the recommendation. The OCIO will coordinate with each system's Program Management Office . . . including the system owners and authorizing officials to help ensure annual testing of the contingency plans in accordance with policy."

Metric 65 – Information System Backup and Storage

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM has implemented processes, strategies, and technologies for information system backup and storage. OPM's systems are backed up to alternative storage sites that are documented within each system's contingency plan.

Metric 66 – Communication of Recovery Activities

FY 2019 Maturity Level: 3 – Consistently Implemented. OPM has polices in place that define how contingency plan activities are performed throughout the agency. As discussed above in Metric 64, OPM distributed these policies and procedures to all relevant stakeholders. However, OPM is not consistently adhering to this policy, as contingency plans are not tested annually for all systems. We received valid contingency plan tests for only 11 percent of OPM's major systems.

For the major OPM systems that were subject to contingency plan testing, OPM produced and distributed the after action reports to the relevant personnel. Those results are used to make risk based decisions.

Metric 67 – Contingency Planning Other Information

There are no additional comments regarding contingency planning.

APPENDIX I – Detailed FISMA Results by Metric

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

Key

Red: Level 1, Ad Hoc

Yellow: Level 2, Defined

Green: Level 3+, Consistently Implemented or higher

APPENDIX II - Status of Prior OIG Audit Recommendations

The table below outlines the current status of recommendations issued in the FY 2018 FISMA audit (Report No. 4A-CI-00-18-038, issued October 30, 2018).

Rec#	Original Recommendation	Recommendation History	Current Status
1	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 Information System Security Officers (ISSOs) to adequately support all of the agency's major information systems.	Rolled forward from FY 2016	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 11
2	We recommend that OPM ensure that the OCIO's senior leadership vacancies are filled and that there is a proper separation of duties for assigned roles and responsibilities.	New recommendation in FY 2018	CLOSED
3	We recommend that all active systems in OPM's inventory have a complete and current Authorization.	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 39
4	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	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 40
5	We recommend that OPM improve the policies and procedures for defining system boundaries and classifying the systems in its environment.	New recommendation in FY 2018	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 1
6	We recommend that the OCIO ensure that all interconnection security agreements are valid and properly maintained.	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 2
7	We recommend that the OCIO ensure that a valid memorandum of understanding/agreement exists for every interconnection.	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 3
8	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	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 5
9	We recommend that OPM define policies and procedures for a centralized software inventory.	New recommendation in FY 2018	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 6

Rec #	Original Recommendation	Recommendation History	Current Status
10	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-00-19-029 Recommendation 7
11	We recommend that OPM define and communicate a risk management strategy based on the requirements outlined in NIST SP 800-39.	Rolled forward from FY 2017	CLOSED
12	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-00-19-029 Recommendation 10
13	We recommend that OPM continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, Section 2.3.2 Risk Executive (Function).	Rolled forward from FY 2011	CLOSED
14	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-00-19-029 Recommendation 12
15	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).	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 13
16	We recommend that OPM complete risk assessments for each major information system that are compliant with NIST guidelines and OPM policy. The results of a complete and comprehensive test of security controls should be incorporated into each risk assessment.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 14
17	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	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 15
18	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	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 16
19	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-00-19-029 Recommendation 17

Rec #	Original Recommendation	Recommendation History	Current Status
20	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-00-19-029 Recommendation 18
21	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-00-19-029 Recommendation 19
22	We recommend that the OCIO conduct routine compliance scans against established baseline configurations for all OPM information systems. This recommendation cannot be addressed until Recommendation 21 has been implemented.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 20
23	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-00-19-029 Recommendation 21
24	We recommend that the OCIO conduct routine compliance scans against [the standard security configuration settings] for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 23 has been completed.	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 22
25	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-00-19-029 Recommendation 23
26	We recommend that the OCIO implement a process to ensure new server installations are included in the scan repository.	New recommendation in FY 2018	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 27
27	We recommend that the OCIO implement a process for updating and maintaining credentials for its scanning accounts.	New recommendation in FY 2018	CLOSED
28	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	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 24
29	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	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 8
30	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	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 25
31	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	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 26

Rec #	Original Recommendation	Recommendation History	Current Status
32	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	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 28
33	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 2016	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 29
34	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	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 30
35	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	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 31
36	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	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 32
37	We recommend that OPM define the roles and responsibilities necessary for the implementation of the agency's privacy program.	New recommendation in FY 2018	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 33
38	We recommend that OPM develop its privacy program by creating the necessary plans, policies, and procedures for the protection of PII.	New recommendation in FY 2018	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 34
39	We recommend that OPM implement controls over encryption of data at rest on its IT systems.	New recommendation in FY 2018	CLOSED
40	We recommend that OPM implement controls over encryption of data in transit on its IT systems.	New recommendation in FY 2018	CLOSED
41	We recommend that OPM develop and implement policies and procedures related to data exfiltration and enhanced network defenses.	New recommendation in FY 2018	CLOSED
42	We recommend that OPM develop a process to routinely test the Data Breach Response Plan.	New recommendation in FY 2018	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 35
43	We recommend that OPM identify individuals with heightened responsibility for PII and provide role-based training to these individuals at least annually.	New recommendation in FY 2018	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 36

Rec #	Original Recommendation	Recommendation History	Current Status
44	We recommend that OPM develop and conduct an assessment of its workforce's knowledge, skills and abilities in order to identify any skill gaps and specialized training needs.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 37
45	We recommend that OPM develop and document a security awareness and training strategy tailored to its mission and risk environment.	Rolled forward from FY 2017	CLOSED
46	We recommend that OPM conduct an analysis to identify any resource gaps within its current ISCM program. OPM should use the results of this gap analysis to ensure stakeholders have adequate resources to effectively implement ISCM activities based on OPM's policies and procedures.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 38
47	We recommend that OPM ensure that an annual test of security controls has been completed for all systems.	Rolled forward from FY 2008	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 41
48	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 47.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 43
49	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.	New recommendation in FY 2018	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 44
50	We recommend that the OCIO conduct an agency-wide BIA and incorporate the results into the system-level contingency plans.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-19-029 Recommendation 45
51	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-00-19-029 Recommendation 46
52	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-00-19-029 Recommendation 47

APPENDIX III

This appendix contains the U.S. Office of Personnel Management's October 3, 2019, response to the draft audit report, issued September 11, 2019.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Chief Information
Officer

October 03, 2019

Memorandum For [redacted]
Chief, Information System Audit Group
Office of the Inspector General

From: Clare A. Martorana
Chief Information Officer
Office of Personnel Management

Subject: Office of Personnel Management Response to the Office of the Inspector General Federal Information Security Modernization Act Audit – FY 2019 (Report No. 4A-CI-00-19-029)

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report, the Federal Information Security Modernization Act (FISMA) Audit for the U.S. Office of Personnel Management (OPM), Report No. 4A-CI-00-19-029. The OIG comments are valuable as they afford us an independent assessment of our operations and help guide our improvements to enhance the security of the data furnished to OPM by the federal workforce, federal agencies, our private industry partners, and the public.

OPM reports that the agency closed eight recommendations in FY 2019, a 15 percent closure rate. This represents the focus we have placed on remediation of the OIG recommendations over the fiscal year. Though OIG added three new recommendations this year, OPM plans to continue to improve our cybersecurity maturity level.

We agree with many of the recommendations made by the OIG. While we do not agree with all of the recommendations made in this report, we appreciate OIG's focus on continued progress toward a fully matured cybersecurity program as set forth by the FISMA maturity model and underlying metrics. This year, OPM concurs with 38 of the OIG's 47 recommendations and respectfully non-concurs or partially concurs with the remaining nine recommendations.

OPM and OIG will continue to work together toward mutual understanding of the use of the evolving FISMA maturity model and its underlying metrics that were first introduced in FY 2017.

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

Recommendation 1 (Rolled forward from 2018): We recommend that OPM improve the policies and procedures for defining system boundaries and classifying the systems in its environment.

Management Response: We concur with the recommendation. OPM considers its policy to be sufficient to meet the intent of the finding as described in the report. However, we are in the process of making revisions to our procedures to align with enhancements to NIST SP 800-37 Revision 2, which will affect how we execute system boundary definitions and system classifications.

Recommendation 2 (Rolled forward from 2014): We recommend that the Office of the Chief Information Officer (OCIO) ensure that all interconnection security agreements are valid and properly maintained.

Management Response: We concur with the recommendation. Early in the fiscal year, several Information System Security Officers (ISSOs) were brought on board with additional contract ISSOs expected to join in the coming months. The OPM CIO completed an ISSO service requirement gap analysis which was a critical component of OCIO efforts to obtain the appropriate funding. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs will be able to address the development and maintenance of interconnection security agreements.

Recommendation 3 (Rolled forward from 2014): We recommend that the OCIO ensure that a valid memorandum of understanding/agreement exists for every interconnection.

Management Response: We concur with the recommendation. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. The OCIO completed an ISSO service requirement gap analysis which was a critical component of OCIO efforts to obtain the appropriate funding. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. The ISSO service model developed in 2019 addresses the development and maintenance of memorandum of understandings/agreements which we anticipate will assist in meeting this metric.

Recommendation 4: We recommend that OPM define the procedures for maintaining its hardware inventory.

Management Response: We concur with the recommendation. In FY 2020, we plan to update

procedures for maintaining the OPM hardware inventory.

Recommendation 5 (Rolled forward from 2016): We recommend that OPM improve its system inventory by correlating the elements of the inventory to the servers and information systems they reside on.

Management Response: We concur with the recommendation. OPM plans to meet this requirement by leveraging toolsets provided by the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program. OPM is in the processing of entering FISMA system boundaries into its CDM tool and is planning to import this data into the Governance, Risk Management, and Compliance (GRC) tool.

Recommendation 6 (Rolled forward from 2018): We recommend that OPM define policies and procedures for a centralized software inventory.

Note: While OPM has defined a policy requiring a centralized software inventory, this recommendation remains open, as the procedures have not been developed.

Management Response: We concur with the recommendation. We plan to expand the OPM Enterprise Change Management (ECM) program, enhance the software inventory, and evaluate the associated reporting and procedures.

Recommendation 7 (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 Response: We concur with the recommendation. We will continue to improve upon the agency's enterprise architecture in FY 2020, specifically regarding the agency software inventory.

Recommendation 8 (Rolled forward from 2016): We recommend that the OCIO implement a process to ensure that only supported software and operating platforms are used within the network environment.

Management Response: We concur with the recommendation. Currently, any time new software is installed on a device, OPM is able to detect the installation. The ECM program will be enhanced to require approval through the ECM process for software installation. We are also actively developing plans to remove unsupported software and operating platforms from the network.

Recommendation 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.

Management Response: We concur with the recommendation. OPM will continue to follow

government-wide guidance and standards to address this recommendation.

Recommendation 10 (Rolled forward from 2017): We recommend that OPM update its enterprise architecture to include the information security architecture elements required by National Institute of Standards and Technology (NIST) and Office of Management and Budget (OMB) guidance.

Management Response: We concur with the recommendation. We will continue to update the enterprise architecture including the necessary information system security architecture. In FY 19 we began the process of updating the enterprise architecture.

Recommendation 11 (Rolled forward from 2016): 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 Information System Security Officers (ISSOs) to adequately support all of the agency's major information systems.

Management Response: We concur with the recommendation. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. The OCIO completed an ISSO service requirement gap analysis which was a critical step to obtain the appropriate resources. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model.

Recommendation 12 (Rolled forward from 2016): We recommend that OPM adhere to remediation dates for its Plan of Action and Milestone (POA&M) weaknesses.

Management Response: We concur with the recommendation. The OCIO prioritized POA&M remediation and management in FY19, recently conducting a POA&M sprint, for example. Efforts to maintain remediation details will continue post-sprint through the use of a new POA&M reporting process and enhanced tools to help us manage the enterprise inventory of POA&Ms. Since we completed our sprint, we have been able to close 36 percent of POA&Ms across the board.

Recommendation 13 (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).

Management Response: We concur with the recommendation. The OCIO has prioritized POA&M remediation and management in FY19, recently conducting a POA&M sprint as previously noted. Efforts to maintain remediation details will continue post-sprint through the use of a new POA&M reporting process and enhanced tools to help us manage the enterprise inventory of POA&Ms. We have improved the POA&M process across the remediation stages with the speed by which they are reviewed and processed. This improvement in speed of

review and processing helps to prevent POA&Ms from missing remediation deadlines.

Recommendation 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.

Management Response: We concur with the recommendation. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. The OCIO completed an ISSO service requirement gap analysis which was a critical step to obtain the appropriate resources. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs will be able to improve the risk assessment metric.

Recommendation 15 (Rolled forward from 2017): 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.

Management Response: We concur with this recommendation. OPM developed requirements for an automated Enterprise Risk Management (ERM) solution. However, OCFO was unable to finalize requirements, conduct acquisition activities, and begin deployment of an ERM solution across OPM programs as enterprise risk management staff was reprioritized to work on transition-related priorities. OCFO was also unable to acquire an enterprise risk management automated tool in FY 2019 due to the lapse in funding and reprioritization. It was and it is still OCFO's goal to implement an automated solution to manage its enterprise risk management program. In FY 2020, the CFO will direct Risk Management and Internal Control (RMIC) to update its plan for the implementation of an ERM solution post transition-related priorities and budget uncertainties.

Recommendation 16 (Rolled forward from 2013): We continue to recommend that the OCIO develop a plan and timeline to enforce the new System Development Life Cycle (SDLC) policy on all of OPM’s system development projects.

Management Response: We concur with the recommendation. We recognize the need to enforce its SDLC policy on all IT projects and plan to implement corrective actions when we can support such activities weighed against other priorities.

Recommendation 17 (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 Configuration Management (CM) program.

Management Response: We concur with the recommendation. We will work to define and

obtain the resource requirements to improve the configuration management program.

Recommendation 18 (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 Response: We do not concur with this recommendation as it is dependent upon the closure of an associated recommendation. Given the gap analysis to be conducted for recommendation 17, which will include best practices based on lessons learned and other factors, this recommendation cannot be countenanced until maturation of the CM program implementation and is thus not timely or appropriate.

Recommendation 19 (Rolled forward from 2107): We recommend that OPM develop and implement a baseline configuration for all information systems in use by OPM.

Management Response: We concur with the recommendation. We are working toward development and implementation of the standard configuration settings for all OPM information systems. We will work towards implementing the standard configuration settings for new deployments of operating platforms through enhancements to its Enterprise Configuration Management process in the upcoming fiscal year.

Recommendation 20 (Rolled forward from 2017): 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 18 has been implemented.

Management Response: We concur with the recommendation. We plan to expand the OPM ECM program to include baseline configuration compliance. We are also considering the feasibility of expanding our change management process to a configuration management process. We will continue to conduct routine compliance scans while adding OPM information systems as is appropriate.

Recommendation 21 (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 Response: We concur with the recommendation. We developed the standard security configuration settings for all OPM operating platforms. We will work towards implementing the standard security configuration settings for new deployments of operating platforms through enhancements to its Enterprise Configuration Management process in the upcoming fiscal year.

Recommendation 22 (Rolled forward from 2017): We recommend that the OCIO conduct

routine compliance scans against [the standard security configuration settings] for all servers and databases in use by OPM.

Note: This recommendation cannot be addressed until Recommendation 20 above has been completed.

Management Response: We concur with the recommendation. We will conduct routine compliance scans against the standard security configuration settings as part of our Enterprise Configuration Management process updates.

Recommendation 23 (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 Response: We concur with the recommendation. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. The OCIO completed an ISSO service requirement gap analysis which was a critical step to obtain the appropriate resources. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs will be able to better document the approval of deviations.

Recommendation 24 (Rolled forward from 2014): We recommend that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.

Management Response: We concur with this recommendation. The process and requirements include the immediate inclusion of the device into OPM's routine scanning repository. OPM controls all devices that are connecting to the network. OPM will produce evidence to support closure of this recommendation in FY 2020.

Recommendation 25 (Rolled forward from 2014): 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.

Management Response: We concur with the recommendation. The OCIO completed an ISSO funding requirement gap analysis which was a critical component of OCIO efforts to obtain the appropriate funding. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. OCIO continues to take steps to hire the adequate number of ISSOs through the ISSO funding model. We believe the ISSOs will be able to effectively track vulnerability scans in POA&Ms.

Recommendation 26 (Rolled forward from 2014): We recommend that the OCIO implement a process to apply operating system and third party vendor patches in a timely manner

Management Response: We concur with the recommendation. OCIO has a process for patch

management to help ensure timely deployment of patches. We have seen significant improvements in patch management timeliness as well as an increase in our ability to deploy patches over the past year. However, going forward, OCIO will work to improve consistency in the area of patch management.

Recommendation 27 (Rolled forward from 2018): We recommend that the OCIO implement a process to ensure new server installations are included in the scan repository.

Management Response: We concur with this recommendation. Projects involving changes to the environment that include new server installations should not be considered complete until this action is completed. We have identified security actions that should be completed based on types of changes that are made in the environment which will be integrated into the change control process. OPM will evaluate further implementation plans in FY 2020.

Recommendation 28 (Rolled forward from 2107): We recommend that OPM conduct an analysis to identify limitations in the current Identity, Credential and Access Management (ICAM) program in order to ensure that stakeholders have adequate resources (people, processes, and technology) to implement the agency's ICAM activities.

Management Response: We concur with this recommendation. While OPM did not previously consider ICAM to be a distinct program, in order to further improve in this metric and meet the intent of OMB Memorandum M-19-17, OPM will work to establish a distinct ICAM program.

Recommendation 29 (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 Response: We concur with this recommendation. While the agency did not previously consider ICAM to be a distinct program, OPM will work to meet the intent of OMB Memorandum M-19-17. We plan to conduct a gap analysis in FY 2020.

Recommendation 30 (Rolled forward from 2017): 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.

Management Response: We concur with this recommendation. While OPM did not previously consider ICAM to be a distinct program, OPM will work to meet the intent of OMB Memorandum M-19-17 and conduct the analysis referenced in Recommendation 29. After Recommendation 29 analysis has been completed, OPM can then address this recommendation to capture and share lessons learned.

Recommendation 31 (Rolled forward from 2012): 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.

Management Response: We concur with the recommendation. OPM will work to meet the intent of OMB Memorandum M-19-17 (which has superseded M-11-11) and revisit plans on how to address this recommendation.

Recommendation 32 (Rolled forward from 2016): 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.

Management Response: We concur with the recommendation. The OCIO has incorporated all contractors into the centralized tool and master user record however processes have not yet been established for routine user account audit or review. OPM relies on support from the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program to support the implementation of these requirements. OPM continues to be at the forefront of working with DHS on the CDM program and will maintain this partnership as CDM evolves.

Recommendation 33 (Rolled forward from 2018): We recommend that OPM define the roles and responsibilities necessary for the implementation of the agency's privacy program.

Response: We do not concur with this recommendation. We disagree that no roles and responsibilities for privacy are currently defined at OPM. The agency has made significant progress toward fully defining the roles and responsibilities for OPM's privacy program to date. The Office of Privacy and Information Management (OPIM) was established in February, 2019, in order to elevate and co-locate certain important and complementary subject matter areas and, in so doing, call attention to their significance in the day-to-day business operations of OPM and to ensure they were properly resourced. This included realigning the former Information Management and Freedom of Information Act (FOIA) groups from the Office of the Chief Information Officer into OPIM and realigning the Chief Privacy Officer/Senior Agency Official for Privacy from within the Office of the Director to lead the new organization. OPIM's key areas of responsibility are: Privacy; FOIA; Records Management; Section 508 Accessibility; Forms Management/Paperwork Reduction Act; and Controlled Unclassified Information (CUI).

Additionally, OPM elevated the Chief Privacy Officer/Senior Agency Official for Privacy (SAOP) to a senior-level position reporting directly to the Director of OPM in 2016. That position, based on the position description and the requirements set forth in guidance from the Office of Management and Budget (Memorandum 16-24) and Executive Order 13719. The SAOP has responsibility for privacy policy and compliance at OPM, and has the necessary authority at the agency to lead and direct OPM's privacy program to carry out the privacy-related functions described in law and OMB policies.

Recommendation 34 (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 Response: We partially concur with this recommendation. We agree that a more focused articulation of privacy policies and procedures that are separate from and/or integrated with information security policy and procedures, is appropriate. The formation of OPIM is the initial step towards that end. We disagree that there are not currently in place plans, policies, and procedures for the protection of PII. The Information Security and Privacy Policy Handbook includes appropriate privacy provisions, as do the current PIA and SORN guides. In addition, the Chief Privacy Officer implemented a robust template for Privacy Impact Assessments (PIA) that has been in use since 2016, as well as a template for Privacy Threshold Analyses (PTA). The PTA template has been implemented both to determine the need for a PIA or a Privacy Act system of records notice and to track appropriate privacy controls as articulated in NIST 800-53, Appendix J. In addition to those OPM-specific policies and procedures, the agency continues to rely on overarching privacy guidance issued by the OMB and NIST. The PIA template follows the prescribed questions required by the eGovernment Act of 2002. The SORN template follows the guidance from OMB Circular A-108. Other documents and templates are being developed in the OPIM office to better enable information management and privacy-related education.

Recommendation 35 (Rolled forward from 2018): We recommend that OPM develop a process to routinely test the Data Breach Response Plan.

Management Response: We concur with this recommendation. We agree that an annual exercise to review the Breach Response Plan can help clarify and refine roles and responsibilities in the event of a breach and help to more clearly articulate the appropriate risk analysis and mitigation steps that should be taken, as provided by the Breach Response Plan and OMB Memorandum 17-12.

Though no formal test of the Data Breach Response Plan has occurred, there have been instances where the OPM Security Operations Center (SOC) routinely informs appropriate OPM personnel when an incident has occurred and steps were taken to address and mitigate any potential harm as appropriate. OPIM staff routinely reviews PII incident reports/breaches received from the SOC and advises the Chief Privacy Office as necessary. The Chief Privacy Officer is a part of the senior members of the OPM staff that routinely meets and interacts with other key members of the workforce, which allows for consistent communication regarding the protection of sensitive identifiable information to occur.

Recommendation 36 (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 Response: We partially concur with this recommendation. We agree that appropriate annual privacy training should be provided. This is done formally through the annual security and privacy awareness training that all individuals at OPM are required to complete. We also agree that it would be beneficial to evaluate more formally whether there are

individuals who, given their job responsibilities and exposure to PII, should receive any additional annual training.

We disagree with the underlying assumption that individuals who regularly handle PII will always require specialized formal annual training. In many instances the annual awareness training, followed by tailored discussions with various offices, can be just as effective. To date, the Chief Privacy Officer has provided presentations on privacy and engaged in group discussions with various offices in an effort to further provide appropriate privacy awareness and compliance.

Recommendation 37 (Rolled forward from 2017): We recommend that OPM develop and conduct an 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 skills gaps and training needs has not been performed.

Management Response: We partially concur with this recommendation. OCIO has adhered to the guidance received and feels it has met the intent of the Federal Cybersecurity Workforce Assessment Act of 2015. OPM will continue to work towards the goals necessary to fulfil specialized training needs.

Recommendation 38 (Rolled forward from 2017): We recommend that OPM conduct an analysis to identify any resource gaps within its current ISCM program. OPM should use the results of this gap analysis to ensure stakeholders have adequate resources to implement ISCM activities effectively based on OPM's policies and procedures.

Management Response: We concur with the recommendation. The OPM CIO completed an ISSO funding requirement gap analysis which was a critical component of OCIO efforts to obtain the appropriate funding. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. OCIO continues to take steps to hire the adequate number of ISSOs through the ISSO funding model.

Recommendation 39 (Rolled forward from 2014): We recommend that all active systems in OPM's inventory have a complete and current Authorization.

Management Response: We partially concur with your recommendation. The OIG found that while OPM had current authorizations for all of its major systems at once point in FY19, six of these authorizations were signed by an agency official no longer with OPM as of issuance of the OIG's draft report. We understand and agree with the need to have a new Authorizing Official re-evaluate authorizations in such circumstances. However, the current NIST guidance in this area permits a range of actions that can be taken including, for example, the signing of a new formal authorization document, reauthorization, or ongoing authorization. With the flexibility afforded agencies in determining how the guidelines will apply, OPM will review

and take appropriate action for authorization packages consistent with updated policies.

Recommendation 40 (Rolled forward from 2014): 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.

Management Response: We partially concur with the recommendation. We have taken, and will continue to take, OIG's recommendation under advisement and agree that system owners provide support to the business processes of the agency. Apart from changes to performance standards, OPM will continue to identify appropriate ways to work with system owners to help ensure FISMA compliance. For instance, recently issued cybersecurity policies set forth expectations and requirements for system owners, consistent with NIST 800 Series guidance.

Recommendation 41 (Rolled forward from 2008): We recommend that OPM ensure that an annual test of security controls has been completed for all systems.

Management Response: We concur with the recommendation. The OCIO completed an ISSO funding requirement gap analysis which was a critical component of OCIO efforts to obtain the appropriate funding. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. OCIO continues to take steps to hire the adequate number of ISSOs through the ISSO funding model.

Recommendation 42: We recommend that OPM define a format for the reports used to communicate the effectiveness of its ISCM program.

Management Response: We do not concur with this recommendation. As noted in the report, OPM identified and defined performance measures. We are collecting and analyzing these performance measures and using our centralized repository tool and associated reporting format. This report format was provided to the OIG upon review of the draft recommendations.

Recommendation 43 (Rolled forward from 2017): 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.

Management Response: We do not concur with this finding. As noted in the report, OPM identified and defined performance measures. We are collecting and analyzing the performance measures based on consistently obtained security assessment control report. Additionally, the agency uses our centralized repository tool reports for evaluation purposes.

Recommendation 44 (Rolled forward from 2018): 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.

Management Response: We concur with the recommendation. The OCIO is aware of the technology and resource gaps related to contingency plan testing. Early in the fiscal year, several ISSOs were brought on board with additional contract ISSOs expected to join in the coming months. The OCIO completed an ISSO service requirement gap analysis which was a critical component of OCIO efforts to obtain the appropriate funding. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs will be able to address gaps in implementation of our contingency planning policy.

Recommendation 45 (Rolled forward from FY 2017): We recommend that the OCIO conduct an agency-wide Business Impact Analysis (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 the results have not been incorporated into the system-level contingency plans.

Management Response: We concur with the recommendation. OPM completed an agency-wide BIA and developed a new template with instructions for incorporating the results into system-level contingency plans in May 2018. The agency expects to see the agency wide BIA results reflected in all contingency plans by the end of FY 2020.

Recommendation 46 (Rolled forward from 2014): We recommend that the OCIO ensure that all of OPM's major systems have contingency plans in place and that they are reviewed and updated annually.

Management Response: We concur with the recommendation. The OCIO will coordinate with each system's Program Management Office (PMO) including the system owners and authorizing officials to help ensure contingency plans are in place and that the annual review and update of the plans occurs in accordance with policy.

Recommendation 47 (Rolled forward from 2008): We recommend that OPM test the contingency plans for each system on an annual basis.

Management Response: We concur with the recommendation. The OCIO will coordinate with each system's Program Management Office (PMO) including the system owners and authorizing officials to help ensure annual testing of the contingency plans in accordance with policy.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact me if you have questions or need additional information.

cc:
Jonathan Blyth
Acting Chief of Staff

Dennis D. Coleman
Chief Financial Officer

Kathleen M. McGettigan
Chief Management Officer

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

Janet L. Barnes
Director, Internal Oversight and Compliance

David Nesting
Deputy Chief Information Officer

Cord E. Chase
Chief Information Security Officer

Tyshawn Thomas
Deputy Chief Human Capital Officer

Mark Robbins
General Counsel

Report Fraud, Waste, and Mismanagement

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

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

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