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 2020

Report Number 4A-CI-00-20-010
October 30, 2020

EXECUTIVE SUMMARY

Federal Information Security Modernization Act Audit - Fiscal Year 2020

Report No. 4A-CI-00-20-010 **October 30, 2020**

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 November 2019 through August 2020 at OPM headquarters in Washington, D.C.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

The Fiscal Year (FY) 2020 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 2020, OPM's cybersecurity maturity level is measured as "2 - Defined."

The following sections provide a high-level outline of OPM's performance in each of the eight domains from the five cybersecurity framework functional areas:

Risk Management – OPM has defined an enterprise-wide risk management strategy through its risk management council. OPM is working to implement a comprehensive inventory management process for its system interconnections, hardware assets, and software.

Configuration Management – OPM continues to develop baseline configurations and approve standard configuration settings for its information systems. The agency is also working to establish routine audit processes to ensure that its systems maintain compliance with 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 a security training strategy and program, and has performed a workforce assessment, but is still working to address gaps identified in its security training needs.

Information Security Continuous Monitoring – OPM has established many of the policies and procedures surrounding continuous monitoring, but the agency has not completed the implementation and enforcement of the policies. OPM also continues to struggle to conduct security controls assessments on all of its information systems.

Incident Response – OPM has implemented many of the required controls for incident response. Based upon our audit work, OPM has successfully implemented all of the FISMA metrics at the level of "consistently implemented" or higher.

Contingency Planning – OPM has not implemented several of the FISMA requirements related to contingency planning, and continues to struggle to maintain its contingency plans as well as conducting contingency plan tests on a routine basis.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
BIA	**Business Impact Analysis**
CDM	**Continuous Diagnostics and Mitigation**
CM	**Configuration Management**
DHS	**U.S. Department of Homeland Security**
ECM	**Enterprise Change Management**
ERM	**Enterprise Risk Management**
FICAM	**Federal Identity, Credential, and Access Management**
FISMA	**Federal Information Security Modernization Act**
FY	**Fiscal Year**
ICAM	**Identity, Credential, and Access Management**
IG	**Inspector General**
IOC	**Internal Oversight and Compliance**
ISCM	**Information Security Continuous Monitoring**
ISSO	**Information System Security Officer**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
OCIO	**Office of the Chief Information Officer**
OMB	**U.S. Office of Management and Budget**
OPIM	**Office of Privacy and Information Management**
OPM	**U.S. Office of Personnel Management**
PII	**Personally Identifiable Information**
PIV	**Personal Identity Verification**
POA&M	**Plan of Action and Milestones**
Q	**Quarter**
SCRM	**Supply Chain Risk Management**
SDLC	**Systems Development Life Cycle**
SP	**Special Publication**

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

ABBREVIATIONS iii

I. **BACKGROUND** 1

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

III. **AUDIT FINDINGS AND RECOMMENDATIONS** 5

A. Introduction and Overall Assessment 5

B. Risk Management 6

C. Configuration Management 19

D. Identity, Credential, and Access Management 27

E. Data Protection and Privacy 33

F. Security Training 38

G. Information Security Continuous Monitoring 40

H. Incident Response 46

I. Contingency Planning 48

APPENDIX I: Detailed FISMA Results by Metric

APPENDIX II: Status of Prior OIG Audit Recommendations

APPENDIX III: The Office of Personnel Management's October 6, 2020, response to the draft audit report, issued September 22, 2020.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

I. BACKGROUND

The 2002 Federal Information Security Management Act requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the U.S. Office of Management and Budget (OMB) on the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. The 2014 Federal Information Security Modernization Act (FISMA) reemphasizes the need for an annual IG evaluation. In accordance with FISMA, we conducted an audit of the U.S. Office of Personnel Management (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 a Chief Information Officer's strategic agency-wide security responsibility. At OPM, security responsibility is assigned to the agency's Office of the Chief Information Officer (OCIO). FISMA also clearly places responsibility on each agency's OCIO to develop, implement, and maintain a security program that assesses risk and provides adequate security for the operations and assets of programs and systems under its control.

To assist agencies and IGs in fulfilling their FISMA evaluation and reporting responsibilities, the U.S. Department of Homeland Security (DHS) Office of Cybersecurity and Communications issued the Fiscal Year (FY) 2020 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 2020 FISMA IG Reporting Metrics utilizing a maturity model evaluation system derived from the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Our audit and reporting approaches were designed in accordance with the issued guidance.

II. 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 two set of controls (OPM's Security Assessment and Authorization process and OPM Common Controls process) and one audit of OPM's major information systems – the Electronic Official Personnel Folder.

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 2020.

We reviewed OPM's general FISMA compliance efforts in the specific areas defined in DHS's guidance and the corresponding reporting instructions. We considered the internal control

structure for various OPM systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls for these various systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. We utilized this understanding to evaluate the degree to which the appropriate internal controls were designed and implemented. As appropriate, we conducted compliance tests using judgmental samples to determine the extent to which established controls and procedures are functioning as required.

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 2020 Inspector General Federal Information Security Modernization Act 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 Guide;
- OMB Circular A-130, Managing Information as a Strategic Resource;
- OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive 12;
- P.L. 107-347, Title III, Federal Information Security Management Act of 2002;

- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- P.L. 115-390, SECURE Technology Act;
- NIST Special Publication (SP) 800-39, Managing Information Security Risk – Organization, Mission, and Information System View;
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems;
- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;
- Federal Cybersecurity Workforce Assessment Act of 2015;
- DHS Federal Emergency Management Agency Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements; and
- Federal Information System Controls Audit Manual.

The OPM Office of the Inspector General, established by the Inspector General Act of 1978, as amended, performed the audit from November 2019 through August 2020 in OPM's Washington, D.C. office.

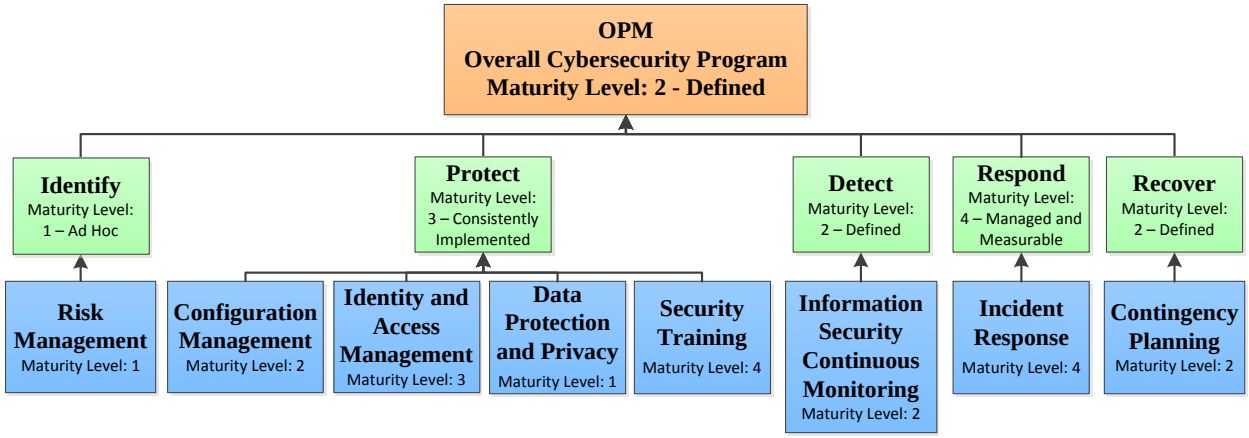
COMPLIANCE WITH LAWS AND REGULATIONS

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 2020 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 cybersecurity control areas used to assess the effectiveness of the information security policies, procedures, and practices of the agency. Each domain is comprised of a series of individual metrics, which are the specific controls that we 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 maturity of OPM's cybersecurity program.

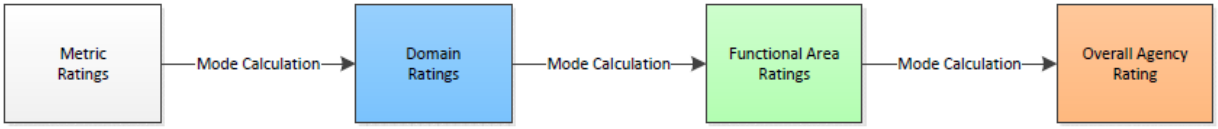


The following table outlines the description of each maturity level rating, as defined by the FY 2020 IG FISMA Reporting Metrics:

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.



The remaining sections of this report provide the detailed results of our audit. 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

FY2020 Maturity Level: 1 – Ad-hoc. OPM has policies and procedures for maintaining an inventory of information systems. These require an interconnection service agreement or memoranda of understanding to be established for system interconnections. OPM operates a centrally maintained tool for managing its system inventory and information.

Although OPM has established a requirement to define system boundaries, a documented process for defining system boundaries does not exist. OPM is piloting a program update to its system registrations, which may include changes to the boundary definition process. However, the scope and timeline for the program are still not defined. Additionally, nine major information systems have a Plan of Action and Milestones (POA&M) to establish the appropriate interconnection agreements.

NIST SP 800-53, Revision 4, advises that an organization "develops and maintains an inventory of its information systems." Furthermore, NIST requires that 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 define and document system boundary and interconnection information increases the risk that OPM senior management does not have adequate system information to determine and identify risk.

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 do not concur with the recommendation. OPM updated its process for defining system boundaries in FY 2020 to align with NIST SP800-37 Revision 2. We implemented a pilot of our process changes in FY 2020 [Quarter (Q)]2 and completed it in FY 2020 Q3. With the successful completion of the pilot we implemented these changes in production for several systems. A briefing was held at that time with OPM Information System Security Managers to outline the changes to the process and convey the updates to the forms being used. We are able to provide the relevant documentation upon OIG request."

OIG Comment:

During fieldwork discussions in FY 2020 Q3, OPM indicated that the pilot program was still in progress. In FY 2020 Q4, OPM responded to the Notice of Finding and Recommendation for this issue stating that progress was being made and offered to provide updates, as available. However, no updated documentation or evidence was subsequently provided. If OPM has updated the policies and procedures for defining system boundaries and classifying the information systems in its environment, we recommend that as part of the audit resolution

process OPM provide OPM's Internal Oversight and Compliance (IOC) office with evidence that the agency implemented this recommendation.

Recommendation 2 (Rolled forward from 2014)

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

OPM Response:

"We concur with the recommendation. OCIO continues to take steps to provide sufficient Information System Security Officer (ISSO) support through the ISSO service model. We believe the ISSOs, when appropriately staffed and funded, will be able to address the development and maintenance of interconnection security agreements."

OIG Comment:

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

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

Recommendation 3 (Rolled forward from 2014)

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

OPM Response:

"We concur with the recommendation. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs, when appropriately staffed and funded, will be able to address the development and maintenance of interconnection security agreements."

Metric 2 – Hardware Inventory

FY2020 Maturity Level: 1 – Ad-hoc. OPM's Security Authorization Guide says that in order to register OPM systems, hardware assets included in its system boundary are documented and electronically maintained. However, OPM does not have a defined process to maintain its

inventory of hardware assets. As a result, hardware inventory does not contain adequate information including location, serial numbers, and system owners. Currently, OPM is working on a project to implement DHS's Continuous Diagnostics and Mitigation program that will include tools to detect hardware. However, the project has not been completed, and the DHS program does not include contractor owned or operated systems.

NIST SP 800-53, Revision 4, states that organizations with centralized inventories must "ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association and information system owner)."

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

Recommendation 4 (Rolled forward from 2019)

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

OPM Response:

"We concur with the recommendation. We will aim 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 has met part of this requirement by purchasing and leveraging toolsets provided by the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program. Also, OPM is in the process of entering FISMA system boundaries into its CDM toolset which will enable mapping of all assets to a FISMA system and inventory reporting capabilities within the OPM CDM Dashboard."

Metric 3 – Software Inventory

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

FY 2020 Maturity Level: 1 – Ad-hoc. OPM has a policy that requires software components to be inventoried. However, a documented process to maintain software inventory is still not in place. Defining data elements to include in a software inventory would improve OPM's tracking of software in its environment. Further, instances of unsupported software were found during our testing. OPM purchased a tool this year that when implemented could address these concerns.

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. Plans to utilize the recently procured Software Asset Management tool have been outlined, and we are in the process of implementing the tool. We are targeting the development of detailed plans in FY 2021, contingent upon continued resources and funding at the current or increased levels."

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. Provided that OCIO resources remain at least at the current levels, we will continue to improve upon the agency's enterprise architecture in FY 2021, specifically regarding the agency software inventory. Subject to available resources, we will first reevaluate the current posture and then develop the remediation plan."

Recommendation 8 (Rolled forward from 2016)

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

OPM Response:

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

Metric 4 – System Security Categorization

FY 2020 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 2020 Maturity Level: 1 – Ad-hoc. OPM's Risk Management and Internal Controls Council manages the Enterprise Risk Management program. The Council meets regularly to discuss various risk topics and update the agencies risk profile. However, OPM has not incorporated supply chain risk management (SCRM) in its risk strategies. OPM has identified funding as an issue in developing an action plan to address supply chain requirements.

The SECURE Technology Act, enacted in December 2018, states, "The head of each executive agency shall be responsible for (1) assessing the supply chain risk posed by the acquisition and use of covered articles and avoiding, mitigating, accepting, or transferring that risk, as appropriate and consistent with the standards, guidelines, and practices identified by the Council under section 1323(a)(1); and (2) prioritizing supply chain risk assessments conducted under paragraph (1) based on the criticality of the mission, system, component, service, or asset."

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

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

Recommendation 9 (Rolled forward from 2019)

We recommend that OPM develop an action plan and outline its processes to address the supply chain risk management requirements of NIST SP 800-161.

OPM Response:

"We concur with the recommendation. OPM will continue to follow government-wide guidance and standards to address this recommendation. OPM's Risk Management Council is awaiting additional guidance from the Federal Acquisition Security Committee, in order to develop a comprehensive strategy and plans."

Metric 6 – Information Security Architecture

FY 2020 Maturity Level: 1 – Ad-hoc. OPM has guidance for implementing an information security architecture. The information security architecture is meant to be a plan for the implementation of security mechanisms. OPM's Enterprise Architecture has not been updated since 2008, and it does not contain a Security Reference Model, which represents the agency's information security architecture. OPM also has an Enterprise Information Security Architecture, however the document is in draft form.

NIST SP 800-53, Revision 4, defines an information security architecture as "An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational subunits, showing their alignment with the enterprise's mission and strategic plans." It also states, "The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes."

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

Recommendation 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. Contingent upon continued resources and funding at the current or increased levels, we are also targeting to hire an Enterprise Architect."

Metric 7 – Risk Management Roles, Responsibilities, and Resources

FY 2020 Maturity Level: 3 – Consistently Implemented. OPM's Cyber Risk Management Strategy defines the roles and responsibilities including the risk management council, chief information security officer, and information system security officers (ISSO). Policies at OPM provide requirements for risk assessments, response, and continuous monitoring.

ISSOs are responsible for conducting risk assessments, developing risk response, and monitoring risk activities of OPM's information systems, as well as addressing some long-standing recommendations. However, OPM continues to struggle to address long-standing recommendations. We were told that turnover within the OCIO is an on-going issue. OCIO has performed gap analysis assessments to address the issue. However, challenges in obtaining all of the necessary approvals in the hiring process has hindered efforts in addressing the identified gaps.

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

Recommendation 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 note that for the Director to be in a position to ensure such an outcome, Congress must provide adequate resources and OMB must allocate them. Subject to that caveat, we concur with the recommendation. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We also recognize that ISSOs alone are not sufficient to adequately operate, secure, and modernize agency IT systems. When appropriately staffed and funded, OPM will work to execute this recommendation remediation."

Metric 8 – Plan of Action and Milestones

FY 2020 Maturity Level: 2 – Defined. POA&Ms are a record of identified weaknesses in OPM information systems controls and are used to track remediation efforts. OPM's OCIO has now prioritized POA&Ms, and stated that a new reporting feature in the POA&M repository alerts system owners of past due POA&Ms. As of July 31, 2020, we still noted the following issues:

More than half of OPM's open POA&Ms have not been updated in over a year.

- 60 percent of open POA&Ms are past due;
- 55 percent have not been updated in over a year; and
- 11 percent have not been updated in three years.

Tracking, updating, remediating, and closing POA&Ms are vital to diagnosing a system's level of risk, which impacts how that system affects the overall risk to OPM. Without up-to-date

POA&Ms, OPM is unable to make effective risk-based decisions and distribute resources efficiently to address risk.

Recommendation 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. OPM has instituted new metrics and processes for reviewing the completion of its POA&Ms which allows for timely awareness of slippage in the POA&M, allowing for corrective action. While we are checking on some potential implementation issues with our tracking tool, we are also manually addressing our POA&Ms. Once any identified issues are addressed, we will be able to provide a more accurate reporting of our POA&M status."

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 should be maintained to track the schedule variance).

OPM Response:

"We concur with the recommendation. OPM has instituted new metrics and processes for reviewing the completion of its POA&Ms which provides for timely awareness of slippage in the POA&M, allowing for corrective action. While we are checking on some potential implementation issues with our tracking tool, we are also manually addressing our POA&Ms and will update the deadlines while working them. Once any identified issues are addressed, we will be able to provide a more accurate reporting of our POA&M status."

Metric 9 – System Level Risk Assessments

FY 2020 Maturity Level: 2 – Defined. OPM has defined policies and procedures for conducting risk assessments on information systems. OPM policy requires that risk assessments be performed periodically, and appropriate response actions be taken to effectively manage risks that have been identified. In 2020, OPM began a project to document the system-level risk assessments in a consistent manner with enterprise wide risk assessments. All new systems will participate in this new process, and existing systems will follow when their annual reviews

occur. However, we have yet to receive any evidence from OPM to indicate that the OCIO's new process to perform risk assessments has been implemented.

OPM policy requires, "All controls selected by the system . . . are assessed" and that "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. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs, when appropriately staffed and funded, will be able to address these concerns."

Metric 10 – Risk Communication

FY2020 Maturity Level: 3 – Consistently implemented. It is the responsibility of the ISSO to discuss risk assessment results with the: System Owner, Authorizing Official, and Chief Information Security Officer. This ensures that information about risks discovered through risk assessments are communicated to all necessary stakeholders in a timely manner. Therefore, OPM is able reduce and potentially eliminate known vulnerabilities in the system through timely communication of risk.

Metric 11 – Contracting Clauses

FY2020 Maturity Level: 3 – Consistently implemented. Policies in place at OPM require the use of specific contract language and service level agreements to ensure contractors meet both Federal and OPM specific standards. Contractors must adhere to required contract language including privacy and security requirements.

Metric 12 – Centralized Enterprise-wide Risk Tool

FY 2020 Maturity Level: 1 – Ad-hoc. OPM does not have a centralized and automated tool to view risk information at the enterprise level. Currently, OPM uses a spreadsheet to track data element requirements of OMB A-123 along with the Enterprise Rise Management playbook. Without a centralized enterprise-wide tool in place at OPM, it is more difficult to understand and determine enterprise-wide risks.

NIST SP 800-39 states that automated monitoring, "should be employed because it is generally faster, more efficient, and more cost-effective than manual monitoring. Automated monitoring is also less prone to human error."

Failure to implement a centralized, automated, enterprise-wide risk management tool increases the risk that information is not captured, current, and/or 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 the recommendation but believe that no further action will be required based on the information provided in this response. The Chief Financial Officer's, Office of Risk Management and Internal Controls manages and oversees the agency's Enterprise Risk Management (ERM) program in accordance with the Office of Management and Budget's (OMB) Circular A-123. This oversight includes the capture, scoring, calibration, prioritization, and monitoring of risks and risk mitigation strategies. Currently, [the Office of Risk Management and Internal Controls] manages the agency's enterprise risk profile and multiple program specific, risk registers. The tracking of risks, remediation efforts, and risk scores is maintained in an automated scoring framework using Microsoft Excel software. The agency scores and tracks risks and risk mitigation efforts based on the recommended criteria in OMB Circular A-123. A copy of the risk profile/automated risk tool was provided to Mr. [redacted], of OPM's Office of Inspector General's (OIG) Information Systems Audit Group, on July 16, 2020. OPM finds its current automated system sufficient to manage the agency's ERM program, as do many agencies government wide who utilize a similar framework to support their ERM efforts. We believe that the current automation tool allows OPM to manage risk information sufficiently, determine risk prioritization through aggregated

scoring, and provide management with the information it needs to develop a greater understanding of agency wide risk based on a strategic review of cross departmental risks.

The current tool includes the following attributes: 1) description of the risk; 2) source of the risk; 3) date the risk was identified; 4) aggregated risk impact score; 5) aggregated risk likelihood score; 6) overall risk score; 7) exposure rating; 8) targeted residual risk score; 9) identified risk mitigation owners; 10) the risk response plan; and 11) post risk mitigation scoring and exposure ratings. Combined with the monthly meetings of the agency's ERM governance body, the Risk Management Council, this tool provides agency leaders with an organization-wide forum to consider all types and sources of risk and prioritize them based on aggregated and calibrated scoring methodologies. We believe that the current tool demonstrates that risk information is captured, current, and being assessed in aggregate."

OIG Comment:

OPM continues to use the same process from prior years for inputting and updating risk information. On July 16, 2020, OPM provided us with a PDF copy of its risk register. However, this document does not show that the agency has implemented an automated enterprise-wide solution for collecting, processing, and displaying risk information.

In response to this recommendation last year, OPM concurred and acknowledged its goal of implementing such an automated system stating, "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." However, if OPM believes that the automated Microsoft Excel spreadsheet referenced above satisfies the intent of this metric and associated recommendation, it should submit a request for closure package to IOC along with relevant evidence.

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

The last update of OPM's System Development Life Cycle (SDLC) policy occurred in 2013, and the policy has still yet to be enforced by the agency for all OPM system development projects. The OCIO responded to the FY 2019 audit recommendation by concurring with the need to enforce its SDLC policy on all IT projects. However, we were also informed by the OCIO that no changes have been made to address this on-going issue.

The Federal Information System Controls Audit Manual guidance 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."

The absence of a consistent 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 adequate IT security controls are not built 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 SDLC policy on all IT projects and plan to implement corrective actions when we can support such activities based upon resources and funding."

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. 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 2020 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 currently have adequate processes and technology to manage its CM program effectively. Additionally, OPM has not allocated the appropriate resources to perform a gap analysis that would assist in identifying areas of concern.

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

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

Recommendation 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 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. When we are able to secure funding and resources, we will work to execute this recommendation remediation."

Metric 15 – Configuration Management Plan

FY 2020 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. The Enterprise Change Management Group prepares a report to track improvements to the ECM program and process based on lessons learned. ECM captures the issues, makes observations, and documents the lessons learned. In addition, it captures mitigations taken. Thus, we believe that there is already a successful

process in place to document lessons learned with regard to configuration management activities."

OIG Comment:

OPM's response to the FY 2019 FISMA Draft Report for the same recommendation stated that this recommendation was inappropriate and not timely. OPM's response stated specifically that the recommendation could not be addressed until the gap analysis from the prior recommendation was completed and a mature CM program fully established at OPM. At no point during the course of this year's audit or in its response to the Notification of Finding and Recommendation has OPM provided policies or procedures that document the lessons learned process. If OPM believes that it has implemented the recommendation, then as part of the audit resolution process we recommend that the OCIO provide IOC with evidence that the agency has implemented this recommendation.

Metric 16 – Implementation of Policies and Procedures

FY 2020 Maturity Level: 2 – Defined. OPM has defined agency-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 in Metrics 17, 18, and 19, below.

Metric 17 – Baseline Configurations

FY 2020 Maturity Level: 1 – Ad-hoc. OPM has not developed a baseline configuration for all of its information systems. NIST SP 800-53, Revision 4, states that "Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to

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

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

NIST SP 800-53, Revision 4, advises that an organization "develops, documents, [and] maintains under configuration control, a current baseline configuration of the information system."

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

Recommendation 19 (Rolled forward from 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 to implement the standard configuration settings for new deployments of operating platforms through enhancements to its Enterprise Configuration Management process in the upcoming fiscal year, based upon funding."

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 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. With additional funding and resources, we will reevaluate the current posture and then develop the remediation plan[.] We will continue to conduct routine compliance scans while adding OPM information systems as is appropriate."

Metric 18 – Security Configuration Settings

FY 2020 Maturity Level: 1 – Ad-Hoc. OPM uses the Defense Information Systems Agency's Security Technical Implementation Guides as the basis for its configuration settings. However, OPM has not consistently implemented the process for documenting and approving exceptions, which means OPM has not customized the configuration settings for its systems and environment. As a result, testing against the Guides is not effective since OPM has not documented 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 effectively 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 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 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 21 above has been completed.

OPM Response:

"We concur with the recommendation. We will aim to 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.

OPM Response:

"We concur with the recommendation. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs, when appropriately staffed and funded, will be able to address these concerns."

Metric 19 – Flaw Remediation and Patch Management

FY 2020 Maturity Level: 2 – Defined. OPM routinely performs automated vulnerability and patch compliance scans on its systems. As a part of our audit testing, we reviewed vulnerability scan results for approximately 120 servers from OPM's server inventory. Our test work indicates that several problems previously identified still exist:

- OPM is not consistently installing all patches in a timely manner; some of the missing patches date back to 2018.

- OPM does not have a formal process to ensure all new devices in the environment are included in the scanning process. We also determined that not every device on OPM's network is scanned routinely.

- OPM does not have a process to record or track the remediation status for routine security weaknesses identified during vulnerability scans. While the agency does distribute vulnerability scan results to system owners to remediate identified weaknesses, formal POA&M entries are only created for weaknesses that require significant time to remediate.

NIST SP 800-53, Revision 4, advises that an organization "Scans for vulnerabilities in the information system and hosted applications . . ." and that the organization "Identifies, reports, corrects information system flaws . . ." and "Installs security-relevant software and firmware updates . . . ."

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."

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

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.

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 establish plans to produce evidence to support closure of this recommendation in FY 2021 Q1."

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.

OPM Response:

"We do not concur with this recommendation. OPM already maintains procedures for conducting vulnerability scans and capturing those results in the Plan of Action and Milestones (POA&M). OPM's policies and procedures with regards to vulnerability management and POA&M management require the application of fixes to identified security flaws within a specified time frame consistent with NIST standards and guidelines. If security fixes are not applied within that time frame, then these controls are determined not to be operating effectively as designed and a POA&M is created to manage the remediation of those flaws that were not fixed in a timely manner. Allowing a time to remediate flaws before a POA&M is created is consistent with NIST standards and guidelines and OMB policy."

OIG Comment:

OPM's policies on scanning have not been updated since 2016, but they do identify that risks are to be documented in POA&Ms if they cannot be fixed in a timely manner. However, historically this process has not been applied to all vulnerabilities identified in scanning. OPM's response to the FY 2019 FISMA Draft Report for this same recommendation concurred with the finding and identified that along with numerous other recommendations, remediation of this recommendation was dependent on having a sufficient number of ISSOs. OPM continues to cite ISSO staffing issues in numerous other responses in this report as an ongoing problem. We were not able to validate that this process was operating effectively during the audit. If OPM believes that all vulnerabilities that cannot be remediated in a timely manner are documented in POA&Ms, then as part of the audit resolution process, we recommend that OPM provide IOC with evidence that the agency has implemented this recommendation.

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.

OPM Response:

"We concur with the recommendation. OCIO has a process for patch management to facilitate the timely deployment of patches. Going forward, OCIO will work to improve

consistency in the patch management processes through improved data collection and strategic process implementation."

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.

OPM Response:

"We concur with this recommendation. The process to ensure new server installations are included on the scan repository, via the ECM, has been developed and is being documented. OPM's full implementation will be completed based upon resources and funding."

Metric 20 – Trusted Internet Connection Program

FY 2020 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 OPM's Capability Validation Report.

Metric 21 – Configuration Change Control Management

FY 2020 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

We have 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 increase security, compliance, interoperability, and customer service. While OPM 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 2020 – Maturity Level: 2 – Defined. OPM has documented policies and procedures that define roles and responsibilities for stakeholders involved in the ICAM program.

Since 2017, we have recommended 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 is working with a contractor to address the process and technology needs of the ICAM program. OPM has not yet defined or assessed the staffing needs of its ICAM governance structure.

The FICAM Roadmap and 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.

Note: OPM has identified the processes and technology necessary to implement the agency's ICAM activities but must assess the governance of their ICAM program with adequate/appropriate staff.

OPM Response:

"We concur with this recommendation. In order to meet the intent of OMB Memorandum M-19-17, OPM will work to establish a distinct ICAM program."

Metric 24 – ICAM Strategy

FY 2020 – Maturity Level: 1 – Ad-Hoc. Last year, we determined that OPM had not developed or implemented an ICAM strategy containing milestones for how the agency plans to align with Federal ICAM initiatives. The ICAM strategy still has not been fully implemented, but OPM has contracted to assess the resource needs of the program. OPM expects to implement its ICAM strategy by June 2021.

According to the FICAM Roadmap and Implementation Guidance, "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."

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

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. OPM will consider its actions to implement this recommendation once a distinct ICAM program is established. This will include a gap analysis from the current state to the 'as-is' assessment."

Metric 25 – Implementation of ICAM Program

FY 2020 Maturity Level: 2 – Defined. OPM has defined policies and procedures for 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 for all systems (Metric 28, below), and does not adequately manage contractor accounts (Metric 32, below).

As explained above, OPM has not yet implemented an ICAM strategy. In addition, OPM has not established an ICAM governance structure and thus cannot capture and share lessons learned on the effectiveness of the ICAM controls.

The FICAM Roadmap and Implementation Guidance 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 being used in an ineffective manner.

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.

OPM Response:

"We concur with this recommendation. OPM will consider its actions to implement this recommendation once a distinct ICAM program is established. This will capture and share lessons learned."

Metric 26 – Personnel Risk

FY 2020 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented processes for assigning personnel risk designations and performing appropriate screenings prior to granting access to its systems. Additionally, OPM re-screens individuals when they change positions or the risk designation of their current position is changed.

Metric 27 – Access Agreements

FY 2020 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented centralized processes for developing, documenting and maintaining access agreements for all users of the network. Users must sign the access agreements prior to gaining any network or systems access. Access agreements are reviewed and re-signed as a part of IT Security and Privacy Awareness training on an annual basis thereafter.

Metric 28 – Multi-factor Authentication with PIV

FY 2020 Maturity Level: 3 – Consistently Implemented. OPM has enforced multi-factor authentication for non-privileged network and remote access using PIV cards. OPM continues to expand its PIV implementation incrementally, but almost half of OPM's major information systems, 23 out of 47, still do not enforce strong authentication mechanisms.

Twenty-three of OPM's major information systems still do not enforce strong authentication mechanisms.

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 currently utilizes PIV authentication to access the OPM network. However, OPM will develop project plans for any of the OPM information systems that currently do not support multi-factor authentication in order to fully implement this requirement. This effort will require the collaboration of and support across all components of OPM, and is resource and funding dependent."

Metric 29 – Strong Authentication Mechanisms for Privileged Users

FY 2020 Maturity Level: 3 – Consistently Implemented. OPM utilizes tools including an enterprise password vault to enforce multi-factor authentication for privileged user access to the OPM network and its back-end servers. Privileged users are also required to use multi-factor authentication to manage Domain Name System records.

Metric 30 – Management of Privileged User Accounts

FY 2020 Maturity Level: 3 – Consistently Implemented. OPM has developed and implemented processes for provisioning, managing, and reviewing user accounts. The OCIO restricts privileged user account functions and restricts session durations. Additionally, the OCIO records, logs, and periodically reviews account sessions. Tools have been implemented to automate some privileged account management processes including password rotation.

Metric 31 – Remote Access Connections

FY 2020 Maturity Level: 4 – Managed and Measurable. OPM has implemented a variety of controls for remote access connections such as the use of approved cryptographic modules, system time outs, and session monitoring. The agency ensures that remote access users' activities are logged and periodically reviewed. If anomalous activity is identified, OPM has the ability to rapidly disconnect remote sessions. In addition, OPM verifies that user devices have been appropriately configured prior to allowing remote access, and restricts the ability of individuals to transfer remotely accessed data to non-authorized devices.

Metric 32 – ICAM Other Information – Contractor Access Management

FY 2020 Maturity Level: Not Applicable, no Longer a FISMA Metric. OPM has defined and implemented processes for managing Federal employees' physical and logical access to sensitive resources. However, OPM does not centrally manage 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.

The Federal Information System Controls Audit Manual 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 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. Additionally, with new staff on board, we will evaluate our current posture and confirm remediation plans by the end of FY 2021 Q3."

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 2020 Maturity Level: 1 – Ad-Hoc. The OPM Information Security and Privacy Policy Handbook continues to be the agency's primary source for data protection and privacy policies. However, this handbook has not been updated since 2011 and does not contain the personally identifiable information (PII) protection plans, policies, and procedures necessary for a mature privacy program. The Chief Privacy Officer position was established in 2016. However, roles and responsibilities for the effective implementation of the agency's privacy program have not been defined. OPM's privacy program is relatively new and has not had sufficient resources devoted to it.

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

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

Recommendation 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. As we noted in last year's FISMA audit response, we disagree with the supposition that no roles and responsibilities for privacy are currently defined. We have previously cited the establishment of the Office of Privacy and Information Management (OPIM) in FY 2019, and have provided the OIG with information regarding how roles and responsibilities have evolved. As resources permit, we will continue to develop and reinforce these roles and responsibilities at the Agency."

OIG Comment:

We acknowledge that OPM has created an office responsible for Privacy at OPM. However, the privacy program continues to rely on roles defined in 2011. The outdated privacy handbook still has the role of Chief Privacy Officer assigned to the CIO specifically. However as noted above, OPM has created a separate position, Chief Privacy Officer, and office, OPIM, for managing privacy controls and implementing the privacy program. As we noted in the FY19 FISMA Final

Report, OPM must define its agency-wide privacy program, not just a single position of responsibility. As such, we continue to recommend that OPM define all of the roles and responsibilities necessary for the implementation of the agency's 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 the recommendation. As noted in previous years, we assert that there are currently in place the necessary policies, plans and procedures to foster privacy compliance and protection of PII. We have previously referenced various OMB memoranda, circulars, guides, documents, and templates in place as generally reliable documents for OPM employees to follow. OPIM staff readily provides guidance to programs and CIO representatives in the course of developing privacy compliance documents. We recognize that more work can be done to update written OPM policies, but severe resource constraints have led us to focus nearly all our efforts on action deliverables required by the e-government, FISMA and OMB Circulars/Memorandums. With the recent approval to hire one additional staff person, we plan to renew our efforts to update documents during Fiscal Year 2021."

OIG Comment:

While we agree that OPM has its privacy handbook from 2011, we noted in the FY 2019 FISMA Final Report that this document does not include the privacy controls detailed by NIST SP 800-53, Revision 4, Appendix J published in 2013, or Circular A-130 published in 2016. Without a detailed policy to follow, systems owners are open to interpret privacy controls as they see convenient. 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 2020 Maturity Level: 3 – Consistently Implemented. OPM has implemented controls to protect sensitive information in its environment. Examples include the use of encryption for systems containing PII and other agency sensitive data both at rest and in transit, controls to prevent and detect untrusted removable media, and controls related to the destruction or reuse of media containing PII or other sensitive agency data.

Metric 35 – Data Exfiltration Prevention

FY 2020 Maturity Level: 4 – Managed and Measurable. OPM has defined policies to prevent data exfiltration from its IT environment and to implement enhanced network defenses. OPM has implemented controls to monitor inbound and outbound network traffic, as well as ensure that all traffic passes through a web content filter. In addition, the Agency has implemented a process to measure the effectiveness of the controls on an ongoing basis.

Metric 36 – Data Breach Response Plan

FY 2020 Maturity Level: 2 – Defined. OPM has defined and communicated its Data Breach Response Plan, including its processes and procedures for data breach notification. As a part of the plan, a Breach Response Team has been established that includes the appropriate agency officials. OPM's breach response plan requires periodic testing and updating. However, this year OPM has not updated or tested its Data Breach Response Plan.

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

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

Recommendation 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. As we noted last year, we agree that an annual exercise to review the Breach Response Plan can help ascertain and perfect roles and responsibilities in the event of a breach and help to improve the risk analysis and appropriate mitigation steps spelled out in OMB Memorandum 17-12 and our own Breach Response Plan. We have not had the resources to be able to sufficiently plan and implement the exercise. While the Breach Response Plan from 2017 remains viable, we also intend to review and update it during the next fiscal year. We also need to emphasize that OPIM staff regularly reviews reports from the Remedy system that identifies potential breaches, and advises the

Chief Privacy Officer as necessary. We follow up with OPM programs as necessary to clarify situations and recommend actions to mitigate any risks identified."

Metric 37 – Privacy Awareness Training

FY 2020 Maturity Level: 1 – Ad-Hoc. OPM administers general privacy-awareness training for all employees as a part of their annual IT security training. OPM policy requires users to "Complete role-based security or privacy training if assigned a significant security or privacy role" and system owners to "Provide role-based security and privacy training to OPM information system users responsible for the operation of security functions/mechanisms for systems under his or her portfolio." However, OPM has not developed role-based privacy training for individuals.

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

OMB Circular A-130 requires agencies to "Provide foundational as well as more advanced levels of security and privacy training to information system users (including managers, senior executives, and contractors) and ensure that measures are in place to test the knowledge level of information system users;" and to "Provide role-based security and privacy training to employees and contractors with assigned security and privacy roles and responsibilities, including managers, before authorizing access to Federal information or information systems or performing assigned duties. . . ."

NIST SP 800-53, Revision 4, Privacy control AR-5 requires an organization: "Administers basic privacy training [Assignment: organization-defined frequency, at least annually] and targeted, role-based privacy training for personnel having responsibility for personally identifiable information (PII) or for activities that involve PII [Assignment: organization-defined frequency, at least annually] . . . ."

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

Failure to provide specific training to individuals with assigned security and privacy roles and responsibilities increases the Agency's risk of improperly implemented controls, which can lead to mishandled data resulting 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 the recommendation. Although we assert that for many of OPM's employees the traditional IT Security and Privacy Awareness Training is sufficient, we support the importance of role-based training for certain specialized employees. In fact, we call this out in our privacy compliance guidance. We query program and CIO representatives in our adjudication of the Privacy Threshold Analysis as to whether role-based training is required for particular program positions and what has been done to accomplish this. Our assessment is that program and support organizations largely understand that role-based training may be needed for various positions and act on it. At our current resource level, we simply do not have the bandwidth to take on any additional responsibilities."

OIG Comment:

We acknowledge that the annual training may be sufficient for some of OPM's employees. However, OPM needs to identify those individuals and roles with heightened responsibilities, which could indicate that additional training is required to implement the required privacy controls and processes at OPM. While we understand that resources are limited, we hope that OPIM can continue to work with the Director to acquire the resources necessary to implement key privacy controls.

Metric 38 – Data Protection and Privacy Other Information

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

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 for the ever-changing risk environment and has made progress in providing tailored training to those with significant security responsibilities. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Security Training domain is "4 – Managed and Measurable."**

Metric 39 – Security Training Policies and Procedures

FY 2020 Maturity Level: 3 – Consistently Implemented. OPM has established an agency-wide IT security awareness training program. Roles and responsibilities for stakeholders are defined and communicated across the agency. OPM continues to mature its security training program by consistently collecting and analyzing performance measures of the training activities.

Metric 40 – Assessment of Workforce

FY 2020 Maturity Level: 2 – Defined. OPM has conducted a gap analysis to determine the knowledge, skills, and abilities of its workforce to determine employees' specialized training needs. OPM has continued to refine its process to implement any training-related strategies agency-wide. OPM will participate in a Federal-wide discussion of skills gaps working with various human resource groups across the government to refine the agency's specialized training strategy. OPM's efforts to tailor the specialized training strategy will allow the agency to update its gap analysis periodically to account for a changing risk environment.

Metric 41 – Security Awareness Strategy

FY 2020 Maturity Level: 2 – Defined. In FY 2020, the security awareness and training strategy has been fully developed to maintain a security awareness program tailored to the mission and risk environment. However, OPM has not consistently implemented its agency-wide security awareness and training strategy as there has been only one gap analysis performed since 2018. As stated in metric 40, a periodic re-assessment should to be performed.

Metric 42 – Specialized Security Training Policies

FY 2020 Maturity Level: 4 –Managed and Measurable. OPM has established policies and procedures that require agency employees to take security awareness and specialized security training. OPM has also implemented a process of tracking metrics related to security awareness and training activities.

Metric 43 – Tracking IT Security Training

FY 2020 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, 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-ups and these are used to update the IT security training program. All of OPM's employees and contractors completed the security awareness training course in FY 2020.

Metric 44 – Tracking Specialized IT Security Training

FY 2020 Maturity Level: 4 – Managed and Measurable. OPM employees with significant information security responsibilities are required to take specialized security training in addition to the annual awareness training. The OCIO uses a database to track the security training taken by employees identified as having security responsibility. One example of the specialized training program involves the OCIO conducting targeted phishing exercises/emails for individuals with security responsibilities, tracking the exercise results, and following up as needed.

Metric 45 – Security Training Other Information

We have 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 2020 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 levels. At the organization and business unit levels, the ISCM Strategy defines how the agency's activities support risk management in accordance with agency 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, to include:

- "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."

As we detail in Metric 49, only 19 of OPM's 47 systems were subject to adequate security controls testing and monitoring in FY 2020.

At this stage in the development of its ISCM program, OPM has not consistently implemented the ISCM strategy and is not meeting its goal of providing stakeholders with sufficient information to evaluate risk.

Metric 47 – ISCM Policies and Procedures

FY 2020 Maturity Level: 2 – Defined. OPM has developed ISCM policies and procedures tailored to OPM's environment including specific requirements and deliverables. However, as discussed in more detail under Metric 49, OPM has not consistently implemented its ISCM policies.

Metric 48 – ISCM Roles, Responsibilities, and Resources

FY 2020 Maturity Level: 2 – Defined. OPM has defined the structure, roles, and responsibilities of its ISCM teams and stakeholders. Last year, OPM conducted an analysis that identified and quantified resource gaps in the ISCM program. This year, OPM has made progress to fill those gaps. However, as discussed in more detail under Metric 49, OPM has not ensured that individuals are consistently performing all of the defined roles and responsibilities.

Metric 49 – Ongoing Security Assessments

FY 2020 Maturity Level: 2 – Defined. OPM has defined its processes for performing ongoing security control assessments, granting system authorizations, and monitoring security controls for individual systems. However, OPM's Security Assessment and Authorization (Authorization) process and testing of security controls are still areas of concern.

1) System Authorizations

System owners are responsible for preparing an Authorization package for review and acceptance by the Authorizing Official. However, OPM policy does not currently address what actions should be taken regarding an information system's Authorization status when an agency official in the Authorization process changes roles or is no longer with the agency.

We reviewed Authorizations for OPM's 47 systems and found that two were signed by agency officials no longer with OPM and three had expired.

NIST SP 800-37, Revision 1, requires that "In the event that there is a change in authorizing officials, the new authorizing official reviews the current Authorization decisions document, Authorization package, and any updated documents created as a result of the ongoing monitoring activities. If the new authorizing official is willing to accept the currently documented risk, then the official signs a new Authorization decision . . . formally [accepting] responsibility and accountability . . . and explicitly accepting the risk . . . ."

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

Recommendation 37 (Rolled forward from 2014)

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

OPM Response:

"We concur with the recommendation. The OIG found that two of OPM's authorizations were signed by an agency official no longer with OPM. We understand and agree with the need to have a new Authorizing Official re-evaluate authorizations in such circumstances. OPM updated its processes using NIST guidance in this area, specifically updating our

Information System Continuous Monitoring strategy. Further details are outlined in the technical comments."

OIG Comment:

OPM's technical response to the draft report included an updated version of its ISCM procedures. The updated procedures contain appropriate guidance for the agency when the Authorizing Official of an information systems changes roles or is no longer with OPM. We recommend that OPM provide IOC with evidence that it is in compliance with the updated procedures.

Recommendation 38 (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 do not concur with the recommendation. We continue to take OIG's recommendation under advisement and agree that system owners provide critical support regarding the security, through the [Authorization] process, for their respective systems. In reviewing the specific recommendation by the OIG, however, and after further analysis was completed, OPM has determined it will take other measures to ensure its system owners focus on the security of their systems. Currently, OCIO has implemented checks and balances to provide system owners with the necessary information in advance of [Authorization]s expiring; and additional analysis is underway to determine if specific training for our system owners is required. Once the analysis is completed OPM will create a plan, including identification of resources – if needed."

OIG Comment:

We continue to see problems year after year in OPM's Authorization process. It continues to be our opinion that modifying system owners' performance standards to include metrics for FISMA compliance for the information systems they own would improve the quality and consistency of system Authorization packages. However, if OPM believes that the "other measures" referenced above will achieve the same intent as our recommendation, then it should provide sufficient evidence to IOC.

2) Controls Testing

OPM policy requires reporting the security status of information systems to the Chief Information Officer for the organization and Authorizing Official for the systems at least quarterly. We reviewed evidence of security control testing for the first two quarters of FY 2020 for OPM's 47 major information systems. Of those, only 19 systems were subject to security controls testing that complied with OPM's requirements for both quarters.

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

Only 19 of OPM's major information systems were subject to security controls compliant with OPM's policy.

By failing to complete a comprehensive security controls test for all information systems, OPM cannot move forward in implementing its ISCM strategy. Furthermore, OPM is at risk of an attack that exploits vulnerabilities that could have been identified by appropriate security controls testing.

Recommendation 39 (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 OCIO efforts to obtain the appropriate funding. OCIO continues to take steps to hire the adequate number of ISSOs through the ISSO funding model."

Metric 50 – Measuring ISCM Program Effectiveness

FY 2020 Maturity Level: 2 – Defined. OPM has identified and defined performance measures and requirements to assess the ISCM program effectiveness, achieve situational awareness, and control ongoing risk. However, OPM is not performing the controls assessments in the ISCM strategy consistently enough to provide meaningful data for measuring 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 consistently capture the performance measures can impede OPM's ability to evaluate the effectiveness of the ISCM program.

Recommendation 40 (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.

OPM Response:

"We do not concur with this finding. OPM provided performance measures during the course of the audit period and has used those measures to maintain situational awareness and make meaningful improvements to the program. Thus, we do not agree that this measure can only be in place after Recommendation 39 is implemented. In fact, OPM measures several areas of its program, not just ongoing control assessments; Recommendation 39 covers just one of the areas of the ISCM program. OPM also uses the data regarding the completion of its tests, as measured under Recommendation 39, as one of its metrics. The lack of consistency for completing assessments as described under Recommendation 39 does not preclude OPM from collecting performance measures or making improvements to the program's effectiveness."

OIG Comment:

Ongoing control assessment has been identified as a problem at OPM for more than a decade. We acknowledge that OPM's ISCM program and ISCM metrics are more than just the ongoing controls assessment. However, the majority of other areas in the ISCM metrics already have recommendations to help OPM improve its security posture, including: hardware and software asset management, configuration and vulnerability management, contingency planning and contingency plan testing, and POA&Ms and Authorizations. In this recommendation, we are focusing on the ongoing controls testing. OPM's ISCM strategy identifies controls testing as one of its objectives stating, "Security controls must be assessed to ensure continued effectiveness of their implementation and operation." and that "Metrics must be defined that provide meaningful indications of the security state of information systems and a path for measurable performance improvements." However, we acknowledge that this recommendation could be implemented

prior to Recommendation 39. If OPM is consistently evaluating the ISCM metrics for ongoing control assessments, then as part of the audit resolution process we recommend that OPM provide IOC with evidence that the agency implemented this recommendation.

Metric 51 – ISCM Other Information

We have 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."**

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

FY 2020 Maturity Level: 4 – Managed and Measureable. OPM's incident response policies, procedures, plans, and strategies have been defined, communicated, and consistently implemented. OPM monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response program and is consistently capturing and sharing lessons learned to implement updates to the program as appropriate.

Metric 53 – Incident Roles and Responsibilities

FY 2020 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 2020 Maturity Level: 3 – Consistently Implemented. OPM utilizes a classification system for its incident response program, allowing the agency to quickly analyze and prioritize any reported or detected incidents. In addition, OPM has implemented several security tools to analyze activity patterns to identify precursors and indicators of security threats to prevent security incidents. OPM is in the process of developing profiling techniques on its networks and systems so that it can more effectively detect security incidents.

Metric 55 – Incident Handling

FY 2020 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 mitigation techniques for exploited vulnerabilities. OPM uses metrics to measure the impact of successful incidents and is quickly able to mitigate related vulnerabilities on other systems so that they are not subject to the same exploitation.

Metric 56 – Sharing Incident Response Information

FY 2020 Maturity Level: 4 – Managed and Measureable. OPM has a documented policy that defines how incident response information will be shared with individuals that have significant security responsibility. There are controls in place to ensure that security incidents are reported to DHS, law enforcement, the OPM OIG, and Congress in a timely manner. OPM has developed and implemented incident response metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.

Metric 57 – Contractual Relationships in Support of Incident Response

FY 2020 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 2020 Maturity Level: 4 – Managed and Measureable. OPM has implemented incident response tools to collect and retain data consistent with the agency's incident response policy, plans, and procedures. OPM utilizes the incident response tools for monitoring and analyzing qualitative and quantitative incident response performance across the agency. OPM uses the data collected from these tools to generate monthly reports for stakeholders on the effectiveness of its incident response program.

Metric 59 – Incident Response Other Information

We have 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 2020 – Maturity Level: 2 – Defined. OPM has a policy describing the agency's contingency planning program roles and responsibilities as well as system-level contingency planning documents that assign individuals to specific recovery activities. We determined that 44 of the 47 systems observed had designated contingency plan response teams to recover systems in the event of a service-impacting incident.

In FY 2019, OPM indicated that staffing constraints led to lapses in contingency plan maintenance and testing. This year we continue to see these constraints affect compliance with OPM policy as only a third of contingency plans were updated as required (see Metric 63 below for additional information) and less than a quarter were tested as required (see Metric 64 below for additional information).

NIST SP 800-34, Revision 1, states that "Recovery personnel should be assigned to . . . teams that will respond to the event, recover capabilities, and return the system to normal operations." Failure to staff critical roles in the contingency planning process increases the risk that OPM will be unable to restore systems to an operational status in the event of a disaster.

Recommendation 41 (Rolled forward from FY 2018)

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

OPM Response:

"We concur with the recommendation. We are aware that there are significant technology and resource gaps related to contingency plan testing. We will aim to complete a gap analysis to document the requirements."

Metric 61 – Contingency Planning Policies and Procedures

FY 2020 – Maturity Level: 2 – Defined. OPM has contingency planning policies and procedures in place, but does not consistently adhere to them. Contingency plans, as well as the contingency planning policy and procedures, are not being reviewed and updated in compliance with OPM policy. In addition, lapses in contingency plan testing have prevented consistent implementation of OPM's lessons learned process, which should serve as the basis for documentation updates and process improvement.

System owners have the responsibility to ensure systems are subject to a contingency plan test each year and that plans are updated accordingly. Failure to manage contingency plans appropriately in a changing environment increases the risk that contingency plans will not help OPM meet 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 longstanding issues at OPM.

Metric 62 – Business Impact Analysis

FY 2020 Maturity Level: 2 – Defined. Identifying an organization's essential mission and the risks facing its business functions is a critical element in developing contingency plans. OPM currently has a process in place to develop a Business Impact Analysis (BIA) at the information system level. Of OPM's 47 major information systems, 35 were determined to have up-to-date BIAs.

In addition, OPM successfully performed an agency-wide BIA in March 2020 as a part of the National Continuity Program. However, OPM has not incorporated the results of this BIA into the system-level contingency plans. It is the responsibility of the system owners and Authorizing Officials to ensure that BIA results are communicated and reflected in system-level contingency plans.

NIST SP 800-53, Revision 4, advises that the agency develop a contingency plan for information systems that "Identifies essential missions and business functions and associated contingency requirements . . . ."

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

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

Recommendation 42 (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. The agency is working towards the requirement to see the agency wide BIA results reflected in all contingency plans."

Metric 63 – Contingency Plan Maintenance

FY 2020 Maturity Level: 2 – Defined. OPM has a policy that requires a contingency plan to be in place and annually updated for every major information system. It is the responsibility of the OCIO 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.

While OPM has made progress, it is still not compliant with this policy. Only 16 of the 47 major systems have contingency plans that were reviewed and updated in FY 2020.

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."

Outdated or inaccurate contingency plans increase the risk that the agency will be unable to restore operations effectively and efficiently in the event of a service-impacting incident.

Recommendation 43 (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 conduct a gap analysis and 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. The required funding and resources must be provided before we are able to effectively implement this remediation."

Metric 64 – Contingency Plan Testing

FY 2020 Maturity Level: 2 – Defined. Routinely testing contingency plans is a critical step in ensuring plans can be executed successfully in the event of a disaster. It is the OCIO's responsibility to coordinate with each system owner and authorizing official to test contingency plans annually in accordance with policy. During our testing only 11 of the 47 systems observed were subject to a contingency plan test in compliance with OPM policy.

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

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

Only 11 of OPM's major information systems were subject to a contingency plan test in accordance with OPM policy.

Recommendation 44 (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 conduct a gap analysis and 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. The required funding and resources must be secured before we are able to effectively implement this remediation."

Metric 65 – Information System Backup and Storage

FY 2020 Maturity Level: 2 - Defined. OPM policy defines controls for data backup, recovery and, testing. System-level contingency plan templates include sections for data backup procedures, alternate processing procedures, and alternate storage site information.

However, we have not received evidence to indicate that OPM performs controls testing to ensure that the alternate storage and processing sites provide information security safeguards equivalent to that of the primary site. We reviewed 17 system security plans and observed that OPM did not consistently document the review of the alternate storage/processing site safeguards.

NIST 800-53, Revision 4, states the organization "Ensures that the alternate storage site provides information security safeguards equivalent to that of the primary site." NIST 800-53, Revision 4, also states the organization "Ensures that the alternate processing site provides information security safeguards equivalent to those of the primary site."

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

Recommendation 45

We recommend that OPM perform and document controls testing to ensure security safeguards for alternate processing and storage sites are equivalent to the primary sites.

OPM Response:

"We do not concur with the recommendation. Security controls are tested as a part of the initial security authorization and on an ongoing basis as defined within the OPM ISCM Plan. We recognize that some of the systems referenced by the OIG have test results that were not considered during the audit and others inherit controls from other systems, including [Federal Risk and Authorization Management Program] cloud service providers. The OCIO is available for continued discussion regarding these control tests, the test results, and additional documentation with the OIG upon request."

OIG Comment:

We acknowledge that OPM policy does require that security controls be tested as a part of an initial Authorization. Our testing focused on existing external systems under OPM's continuous monitoring process to ensure that controls continue to be in place and effective after an initial authorization. OPM's ISCM Strategy states, "Due to the restrictions on OPM's capabilities to timely monitor and report on the status of the security posture of externally hosted information systems … a zero-base review must be conducted on externally hosted information systems at least every three years." It also defines a zero-base review stating, "The zero-base review includes an assessment of all implemented security controls from the information SSP." For conducting control assessments OPM' Authorization guidance states, "Each control that is inherited from the [cybersecurity common controls] or another system will validate the accuracy of inheritance." During the course of the audit, we were unable to verify that security controls at alternate sites were adequately tested. At a minimum, the controls testing documentation should validate the control inheritance. As such, we continue to recommend that OPM perform and document controls testing to ensure security safeguards for alternate processing and storage sites are equivalent to the primary sites. If OPM believes that it is consistently evaluating security controls at its systems' alternate sites, then as part of the audit resolution process, we recommend that OPM provide IOC with evidence that the agency implemented this recommendation.

Metric 66 – Communication of Recovery Activities

FY 2020 Maturity Level: 2 – Defined. OPM has defined the process for communicating results of recovery activities to stakeholders in policies and procedures. At the conclusion of a contingency plan test or significant service-impacting incident, results are to be communicated to stakeholders in the form of an after action report. However, OPM is not adhering to this policy, as contingency plans are not tested annually for all systems. We received valid contingency plan tests for only 11 of the 47 systems observed.

OPM was able to produce some completed after action reports that had been shared, but without the required testing, there is not sufficient evidence to prove that the control is consistently implemented.

Metric 67 – Contingency Planning Other Information

We have no additional comments regarding contingency planning.

APPENDIX I – Detailed FISMA Results by Metric

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

KEY

Red – Ad Hoc

Yellow – Defined

Green – Consistently Implemented or higher

APPENDIX II – Status of Prior OIG Audit Recommendations

The table below outlines the current status of recommendations issued in the FY 2019 FISMA audit (Report No. 4A-CI-00-19-029, issued October 29, 2019).

1	We recommend that OPM improve the policies and procedures for defining system boundaries and classifying the systems in its environment.	Rolled forward from FY 2018	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 1
2	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-00-20-010 Recommendation 2
3	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-00-20-010 Recommendation 3
4	We recommend that OPM define the procedures for maintaining its hardware inventory.	New recommendation in FY 2019	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 4
5	We recommend that OPM improve its system inventory by correlating the elements of the inventory to the servers and information systems they reside on.	Rolled forward from FY 2016	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 5
6	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.	Rolled forward from FY 2018	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 6
7	We recommend that OPM define the standard data elements for an inventory of software assets and licenses with the detailed information necessary for tracking and reporting, and that it update its software inventory to include these standard data elements.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 7
8	We recommend that the OCIO implement a process to ensure that only supported software and operating platforms are used within the network environment.	Rolled forward from FY 2016	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 8
9	We recommend that OPM develop an action plan and outline its processes to address the supply chain risk management requirements of NIST SP 800-161.	New recommendation in FY 2019	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 9
10	We recommend that OPM update its enterprise architecture, to include the information security architecture elements required by NIST and OMB guidance.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 10
11	We recommend that the OPM Director ensure that the OCIO has sufficient resources to adequately operate, secure, and modernize agency IT systems.	Rolled forward from FY 2016	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 11

	We also recommend that the agency hire a sufficient number of ISSOs to adequately support all of the agency's major information systems.		
12	We recommend that OPM adhere to remediation dates for its POA&M weaknesses.	Rolled forward from FY 2016	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 12
13	We recommend that OPM update the remediation deadline in its POA&Ms when the control weakness has not been addressed by the originally scheduled deadline (i.e., the POA&M deadline should not reflect a date in the past and the original due date should be maintained to track the schedule variance).	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 13
14	We recommend that OPM complete risk assessments for each major information system that are compliant with NIST guidelines and OPM policy. The results of a complete and comprehensive test of security controls should be incorporated into each risk assessment.	New recommendation in FY 2019	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 14
15	We recommend that OPM identify and define the requirements for an automated enterprise-wide solution for tracking risks, remediation efforts, dependencies, risk scores, and management dashboards, and implement the automated enterprise-wide solution.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 15
16	We continue to recommend that the OCIO develop a plan and timeline to enforce the new SDLC policy on all of OPM's system development projects.	Rolled forward from FY 2013	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 16
17	We recommend that OPM perform a gap analysis to determine the configuration management resource requirements (people, processes, and technology) necessary to effectively implement the agency's CM program.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 17
18	We recommend that OPM document the lessons learned from its configuration management activities and update its configuration management plan as appropriate.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 18
19	We recommend that OPM develop and implement a baseline configuration for all information systems in use by OPM.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 19
20	We recommend that the OCIO conduct routine compliance scans against established baseline configurations for all OPM information systems. Note: This recommendation cannot be addressed until Recommendation 19 has been implemented.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 20
21	We recommend that the OCIO develop and implement [standard security configuration settings] for all operating platforms in use by OPM.	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 21

22	We recommend that the OCIO conduct routine compliance scans against [the standard security configuration settings] for all servers and databases in use by OPM. Note: This recommendation cannot be addressed until Recommendation 20 above has been completed.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 22
23	For OPM configuration standards that are based on a pre-existing generic standard, we recommend that OPM document all instances where the OPM-specific standard deviates from the recommended configuration setting.	Rolled forward from FY 2016	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 23
24	We recommend that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 24
25	We recommend that the OCIO implement a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 25
26	We recommend that the OCIO implement a process to apply operating system and third party vendor patches in a timely manner.	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 26
27	We recommend that the OCIO implement a process to ensure new server installations are included in the scan repository.	Rolled forward from FY 2018	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 27
28	We recommend that OPM conduct an analysis to identify limitations in the current ICAM program in order to ensure that stakeholders have adequate resources (people, processes, and technology) to implement the agency's ICAM activities.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 28
29	We recommend that OPM develop and implement an ICAM strategy that considers a review of current practices ("as-is" assessment) and the identification of gaps (from a desired or "to-be" state), and contains milestones for how the agency plans to align with Federal ICAM initiatives.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 29
30	We recommend that OPM implement a process to capture and share lessons learned on the effectiveness of its ICAM policies, procedures, and processes to update the program.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 30
31	We recommend that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials. 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	Rolled forward from FY 2012	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 31

	forward the recommendation as the new guidance still requires OPM to update its major information systems to require multi-factor authentication using PIV credentials.		
32	We recommend that the OCIO maintain a centralized list of all contractors that have access to the OPM network and use this list to routinely audit all user accounts for appropriateness.	Rolled forward from FY 2016	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 32
33	We recommend that OPM define the roles and responsibilities necessary for the implementation of the agency's privacy program.	Rolled forward from FY 2018	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 33
34	We recommend that OPM develop its privacy program by creating the necessary plans, policies, and procedures for the protection of PII.	Rolled forward from FY 2018	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 34
35	We recommend that OPM develop a process to routinely test the Data Breach Response Plan.	Rolled forward from FY 2018	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 35
36	We recommend that OPM identify individuals with heightened responsibility for PII and provide role-based training to these individuals at least annually.	Rolled forward from FY 2018	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 36
37	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.	Rolled forward from FY 2017	Support Closure
38	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.	Rolled forward from FY 2017	Support Closure
39	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-00-20-010 Recommendation 37
40	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-00-20-010 Recommendation 38
41	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-00-20-010 Recommendation 39
42	We recommend that OPM define a format for the reports used to communicate the effectiveness of its ISCM program.	New recommendation in FY 2019	Support Closure

43	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.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 40
44	We recommend that OPM perform a gap-analysis to determine the contingency planning requirements (people, processes, and technology) necessary to effectively implement the agency's contingency planning policy.	Rolled forward from FY 2018	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 41
45	We recommend that the OCIO conduct an agency-wide BIA and incorporate the results into the system-level contingency plans. Note: While OPM has performed an agency wide BIA, this recommendation remains open, as OPM has not incorporated the results into the system-level contingency plans.	Rolled forward from FY 2017	OPEN: Rolled forward as Report 4A-CI-00-20-010 Recommendation 42
46	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-00-20-010 Recommendation 43
47	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-00-20-010 Recommendation 44

APPENDIX III

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Chief Information
Officer

October 6, 2020

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

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

Through: Kellie Cosgrove Riley
Chief Privacy Officer
Office of Privacy and Information Management
Office of Personnel Management

Subject: Office of Personnel Management Response to the Office of the Inspector General Federal Information Security Modernization Act Audit – FY 2020
(Report No. 4A-CI-00-20-010)

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-00-20-010. The OIG comments are valuable as they afford us an independent assessment of our operations and help inform our continuous efforts to enhance the security of the data furnished to OPM by the federal workforce, federal agencies, private industry, and the public.

OPM reports that the agency closed three recommendations in FY 2020, a six percent closure rate. While this is a smaller percentage than last year, we have continued to prioritize and remediate the OIG recommendations over the fiscal year with efficiency and purpose working within our funding and resources.

We agree with many of the recommendations made by the OIG and we appreciate OIG's focus on continued progress toward a fully matured cybersecurity and privacy posture as set forth by the FISMA maturity model and underlying metrics. This year, OPM concurs with

OIG's 45 recommendations and respectfully non-concurs or partially concurs with the remaining 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 which 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 do not concur with the recommendation. OPM updated its process for defining system boundaries in FY 2020 to align with NIST SP800-37 Revision 2. We implemented a pilot of our process changes in FY 2020 Q2 and completed it in FY 2020 Q3. With the successful completion of the pilot we implemented these changes in production for several systems. A briefing was held at that time with OPM Information System Security Managers to outline the changes to the process and convey the updates to the forms being used. We are able to provide the relevant documentation upon OIG request.

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. OCIO continues to take steps to provide sufficient Information System Security Officer (ISSO) support through the ISSO service model. We believe the ISSOs, when appropriately staffed and funded, 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. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs, when appropriately staffed and funded, will be able to address the development and maintenance of interconnection security agreements.

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

Management Response: We concur with the recommendation. We will aim 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 has met part of this requirement by purchasing and leveraging toolsets provided by the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program. Also, OPM is in the process of entering FISMA system boundaries into its CDM toolset which will enable mapping of all assets to a FISMA system and inventory reporting capabilities within the OPM CDM Dashboard.

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

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. Plans to utilize the recently procured Software Asset Management tool have been outlined, and we are in the process of implementing the tool. We are targeting the development of detailed plans in FY 2021, contingent upon continued resources and funding at the current or increased levels.

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. Provided that OCIO resources remain at least at the current levels, we will continue to improve upon the agency's enterprise architecture in FY 2021, specifically regarding the agency software inventory. Subject to available resources, we will first reevaluate the current posture and then develop the remediation plan.

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. The ECM program and processes require approval for software installation. Additionally, any time new software is installed on a device, OPM is able to detect the installation. We are also actively developing plans to remove unsupported software and operating platforms from the network.

Recommendation 9 (Rolled forward from 2019): We recommend that OPM develop an action plan and outline its processes to address the supply chain risk management requirements of NIST SP 800-161.

Management Response: We concur with the recommendation. OPM will continue to follow government-wide guidance and standards to address this recommendation. OPM's Risk

Management Council is awaiting additional guidance from the Federal Acquisition Security Committee, in order to develop a comprehensive strategy and plans.

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.

Management Response: We concur with the recommendation. We will continue to update the enterprise architecture including the necessary information system security architecture. Contingent upon continued resources and funding at the current or increased levels, we are also targeting to hire an Enterprise Architect.

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.

Management Response: We note that for the Director to be in a position to ensure such an outcome, Congress must provide adequate resources and OMB must allocate them. Subject to that caveat, we concur with the recommendation. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We also recognize that ISSOs alone are not sufficient to adequately operate, secure, and modernize agency IT systems. When appropriately staffed and funded, OPM will work to execute this recommendation remediation.

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. OPM has instituted new metrics and processes for reviewing the completion of its POA&Ms which allows for timely awareness of slippage in the POA&M, allowing for corrective action. While we are checking on some potential implementation issues with our tracking tool, we are also manually addressing our POA&Ms. Once any identified issues are addressed, we will be able to provide a more accurate reporting of our POA&M status.

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 should be maintained to track the schedule variance).

Management Response: We concur with the recommendation. OPM has instituted new metrics and processes for reviewing the completion of its POA&Ms which provides for timely awareness of slippage in the POA&M, allowing for corrective action. While we are checking on some potential implementation issues with our tracking tool, we are also manually addressing our POA&Ms and will update the deadlines while working them. Once any

identified issues are addressed, we will be able to provide a more accurate reporting of our POA&M status.

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.

Management Response: We concur with the recommendation. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs, when appropriately staffed and funded, will be able to address these concerns.

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 the recommendation but believe that no further action will be required based on the information provided in this response. The Chief Financial Officer's, Office of Risk Management and Internal Controls (RMIC) manages and oversees the agency's Enterprise Risk Management (ERM) program in accordance with the Office of Management and Budget's (OMB) Circular A-123. This oversight includes the capture, scoring, calibration, prioritization, and monitoring of risks and risk mitigation strategies. Currently, RMIC manages the agency's enterprise risk profile and multiple program specific, risk registers. The tracking of risks, remediation efforts, and risk scores is maintained in an automated scoring framework using Microsoft Excel software. The agency scores and tracks risks and risk mitigation efforts based on the recommended criteria in OMB Circular A-123. A copy of the risk profile/automated risk tool was provided to Mr. Scott Terry, of OPM's Office of Inspector General's (OIG) Information Systems Audit Group, on July 16, 2020. OPM finds its current automated system sufficient to manage the agency's ERM program, as do many agencies government wide who utilize a similar framework to support their ERM efforts. We believe that the current automation tool allows OPM to manage risk information sufficiently, determine risk prioritization through aggregated scoring, and provide management with the information it needs to develop a greater understanding of agency wide risk based on a strategic review of cross departmental risks.

The current tool includes the following attributes: 1) description of the risk; 2) source of the risk; 3) date the risk was identified; 4) aggregated risk impact score; 5) aggregated risk likelihood score; 6) overall risk score; 7) exposure rating; 8) targeted residual risk score; 9) identified risk mitigation owners; 10) the risk response plan; and 11) post risk mitigation scoring and exposure ratings. Combined with the monthly meetings of the agency's ERM governance body, the Risk Management Council, this tool provides agency leaders with an organization-wide forum to consider all types and sources of risk and prioritize them based on aggregated and calibrated scoring methodologies. We believe that the current tool demonstrates that risk information is captured, current, and being assessed in aggregate.

Recommendation 16 (Rolled forward from 2013): We continue to recommend that the OCIO develop a plan and timeline to enforce the new SDLC [System Development Life Cycle] policy on all of OPM's system development projects.
Management Response: We concur with the recommendation. We recognize the need to enforce SDLC policy on all IT projects and plan to implement corrective actions when we can support such activities based upon resources and funding.

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 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. When we are able to secure funding and resources, we will work to execute this recommendation remediation.

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. The Enterprise Change Management Group prepares a report to track improvements to the ECM program and process based on lessons learned. ECM captures the issues, makes observations, and documents the lessons learned. In addition, it captures mitigations taken. Thus, we believe that there is already a successful process in place to document lessons learned with regard to configuration management activities.

Recommendation 19 (Rolled forward from 2017): 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 to implement the standard configuration settings for new deployments of operating platforms through enhancements to its Enterprise Configuration Management process in the upcoming fiscal year, based upon funding.

Recommendation 20 (Rolled forward from 2017): We recommend that the OCIO conduct routine compliance scans against established baseline configurations for all OPM information systems.

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. With additional funding and resources, we will reevaluate the current posture and then develop the remediation plan 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.

Management Response: We concur with the recommendation. We will aim to 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. OCIO continues to take steps to provide sufficient ISSO support through the ISSO service model. We believe the ISSOs, when appropriately staffed and funded, will be able to address these concerns.

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 establish plans to produce evidence to support closure of this recommendation in FY 2021 Q1.

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 do not concur with this recommendation. OPM already maintains procedures for conducting vulnerability scans and capturing those results in the Plan of Action and Milestones (POA&M). OPM's policies and procedures with regards to vulnerability management and POA&M management require the application of fixes to identified security flaws within a specified time frame consistent with NIST standards and guidelines. If security fixes are not applied within that time frame, then these controls are determined not to be operating effectively as designed and a POA&M is created to manage the remediation of those

flaws that were not fixed in a timely manner. Allowing a time to remediate flaws before a POA&M is created is consistent with NIST standards and guidelines and OMB policy.

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 facilitate the timely deployment of patches. Going forward, OCIO will work to improve consistency in the patch management processes through improved data collection and strategic process implementation.

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. The process to ensure new server installations are included on the scan repository, via the ECM, has been developed and is being documented. OPM's full implementation will be completed based upon resources and funding.

Recommendation 28 (Rolled forward from 2107): 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.

Management Response: We concur with this recommendation. In order to 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. OPM will consider its actions to implement this recommendation once a distinct ICAM program is established. This will include a gap analysis from the current state to the "as-is" assessment.

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. OPM will consider its actions to implement this recommendation once a distinct ICAM program is established. This will 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.

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.

Management Response: We concur with the recommendation. OPM currently utilizes PIV authentication to access the OPM network. However, OPM will develop project plans for any of the OPM information systems that currently do not support multi-factor authentication in order to fully implement this requirement. This effort will require the collaboration of and support across all components of OPM, and is resource and funding dependent.

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. Additionally, with new staff on board, we will evaluate our current posture and confirm remediation plans by the end of FY 2021 Q3.

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.

Management Response: We do not concur with this recommendation. As we noted in last year's FISMA audit response, we disagree with the supposition that no roles and responsibilities for privacy are currently defined. We have previously cited the establishment of the Office of Privacy and Information Management (OPIM) in FY 2019, and have provided the OIG with information regarding how roles and responsibilities have evolved. As resources permit, we will continue to develop and reinforce these roles and responsibilities at the Agency.

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 the recommendation. As noted in previous years, we assert that there are currently in place the necessary policies, plans and procedures to foster privacy compliance and protection of PII. We have previously referenced various OMB memoranda, circulars, guides, documents, and templates in place as generally reliable documents for OPM employees to follow. OPIM staff readily provides guidance to programs

and CIO representatives in the course of developing privacy compliance documents. We recognize that more work can be done to update written OPM policies, but severe resource constraints have led us to focus nearly all our efforts on action deliverables required by the e-government, FISMA and OMB Circulars/Memorandums. With the recent approval to hire one additional staff person, we plan to renew our efforts to update documents during Fiscal Year 2021.

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. As we noted last year, we agree that an annual exercise to review the Breach Response Plan can help ascertain and perfect roles and responsibilities in the event of a breach and help to improve the risk analysis and appropriate mitigation steps spelled out in OMB Memorandum 17-12 and our own Breach Response Plan. We have not had the resources to be able to sufficiently plan and implement the exercise. While the Breach Response Plan from 2017 remains viable, we also intend to review and update it during the next fiscal year. We also need to emphasize that OPIM staff regularly reviews reports from the Remedy system that identifies potential breaches, and advises the Chief Privacy Officer as necessary. We follow up with OPM programs as necessary to clarify situations and recommend actions to mitigate any risks identified.

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 the recommendation. Although we assert that for many of OPM's employees the traditional IT Security and Privacy Awareness Training is sufficient, we support the importance of role-based training for certain specialized employees. In fact, we call this out in our privacy compliance guidance. We query program and CIO representatives in our adjudication of the Privacy Threshold Analysis as to whether role-based training is required for particular program positions and what has been done to accomplish this. Our assessment is that program and support organizations largely understand that role-based training may be needed for various positions and act on it. At our current resource level, we simply do not have the bandwidth to take on any additional responsibilities.

Recommendation 37 (Rolled forward from 2014): We recommend that all active systems in OPM's inventory have a complete and current Authorization.

Management Response: We concur with the recommendation. The OIG found that two of OPM's authorizations were signed by an agency official no longer with OPM. We understand and agree with the need to have a new Authorizing Official re-evaluate authorizations in such circumstances. OPM updated its processes using NIST guidance in this area, specifically updating our Information System Continuous Monitoring strategy. Further details are outlined in the technical comments.

Recommendation 38 (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 do not concur with the recommendation. We continue to take OIG's recommendation under advisement and agree that system owners provide critical support regarding the security, through the ATO process, for their respective systems. In reviewing the specific recommendation by the OIG, however, and after further analysis was completed, OPM has determined it will take other measures to ensure its system owners focus on the security of their systems. Currently, OCIO has implemented checks and balances to provide system owners with the necessary information in advance of ATOs expiring; and additional analysis is underway to determine if specific training for our system owners is required. Once the analysis is completed OPM will create a plan, including identification of resources – if needed.

Recommendation 39 (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. OCIO continues to take steps to hire the adequate number of ISSOs through the ISSO funding model.

Recommendation 40 (Rolled forward from 2017): We recommend that OPM evaluate qualitative and quantitative performance measures on the performance of its information system continuous monitoring (ISCM) program once it can consistently acquire security assessment results, as referenced in recommendation 39.

Management Response: We do not concur with this finding. OPM provided performance measures during the course of the audit period and has used those measures to maintain situational awareness and make meaningful improvements to the program. Thus, we do not agree that this measure can only be in place after Recommendation 39 is implemented. In fact, OPM measures several areas of its program, not just ongoing control assessments; Recommendation 39 covers just one of the areas of the ISCM program. OPM also uses the data regarding the completion of its tests, as measured under Recommendation 39, as one of its metrics. The lack of consistency for completing assessments as described under Recommendation 39 does not preclude OPM from collecting performance measures or making improvements to the program's effectiveness.

Recommendation 41 (Rolled forward from 2018): We recommend that OPM perform a gap-analysis to determine the contingency planning requirements (people, processes, and technology) necessary to implement the agency's contingency planning policy effectively.

Management Response: We concur with the recommendation. We are aware that there are significant technology and resource gaps related to contingency plan testing. We will aim to complete a gap analysis to document the requirements.

Recommendation 42 (Rolled forward from FY 2017): We recommend that the OCIO conduct an agency-wide BIA and incorporate the results into the system-level contingency plans.

Note: While OPM has performed an agency wide BIA, this recommendation remains open, as OPM has not incorporated the results into the system-level contingency plans.

Management Response: We concur with the recommendation. The agency is working towards the requirement to see the agency wide BIA results reflected in all contingency plans.

Recommendation 43 (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 conduct a gap analysis and 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. The required funding and resources must be provided before we are able to effectively implement this remediation.

Recommendation 44 (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 conduct a gap analysis and 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. The required funding and resources must be secured before we are able to effectively implement this remediation.

Recommendation 45: We recommend that OPM perform and document controls testing to ensure security safeguards for alternate processing and storage sites are equivalent to the primary sites.

Management Response: We do not concur with the recommendation. Security controls are tested as a part of the initial security authorization and on an ongoing basis as defined within the OPM ISCM Plan. We recognize that some of the systems referenced by the OIG have test results that were not considered during the audit and others inherit controls from other systems, including FedRAMP cloud service providers. The OCIO is available for continued discussion regarding these control tests, the test results, and additional documentation with the OIG upon request.

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:
Basil Parker
Chief of Staff

Dennis D. Coleman
Chief Financial Officer

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

Janet L. Barnes
Director, Internal Oversight and Compliance

Guy Cavallo
Principal Deputy CIO

David Nesting
Deputy Chief Information Officer

Cord E. Chase
Chief Information Security Officer

Darrin McConnell
Deputy Chief Information Security 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