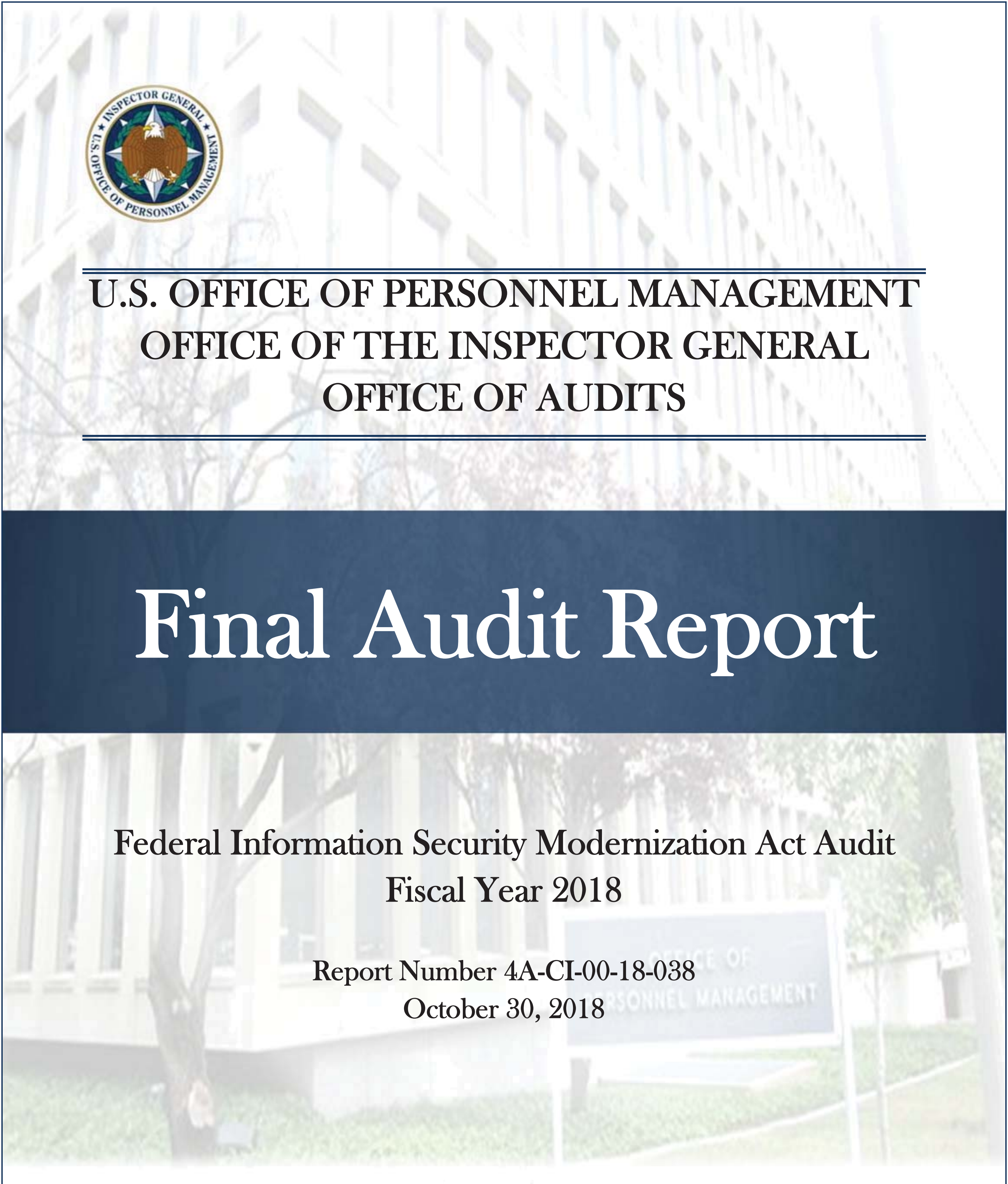


U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Federal Information Security Modernization Act Audit
Fiscal Year 2018

Report Number 4A-CI-00-18-038
October 30, 2018

EXECUTIVE SUMMARY

Federal Information Security Modernization Act Audit - Fiscal Year 2018

Report No. 4A-CI-00-18-038 **October 30, 2018**

Why Did We Conduct the Audit?

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

What Did We Audit?

The OPM Office of the Inspector General has completed a performance audit of OPM's general FISMA compliance efforts in the areas defined in DHS's guidance and the corresponding reporting instructions. Our audit was conducted from April through September 2018 at OPM headquarters in Washington, D.C.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

The Fiscal Year (FY) 2018 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 2018, OPM's cybersecurity maturity level is measured as "2 - Defined."

In addition, OPM's information security governance program has been a longstanding concern. We have assessed it to be a material weakness or a significant deficiency in OPM's internal control structure since FY 2007. This year, we again consider deficiencies in the agency's information security governance program to be a material weakness in the agency's IT security internal control structure. A lack of resources dedicated to IT operations and the agency's culture of minimizing the role of the Chief Information Officer are primary factors causing these issues.

Like OPM's IT security governance program, we have reported either a material weakness or a significant deficiency in OPM's security assessment and authorization process since FY 2014 because of incomplete, inconsistent, and sub-par work products. This year we believe that the current control weaknesses are less severe than a material weakness, but are still a significant deficiency in IT security controls. While there appears to be a valid security assessment and authorization in place for almost every major IT system in the agency's system inventory, the quality of the work and supporting documentation is questionable.

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

Risk Management – OPM is working to implement a comprehensive inventory management process for its system interconnections, hardware assets, and software. OPM is also working to establish a risk executive function that will help ensure that risk assessments are completed and risk is communicated throughout the organization.

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

Identity, Credential, and Access Management (ICAM) – OPM is continuing to improve upon its program by establishing an agency ICAM strategy, and ensuring that an auditing process is implemented for all contractor access.

Data Protection and Privacy – OPM has not implemented several of the FISMA requirements related to data protection and privacy. This is a new domain area for the FY 2018 FISMA metrics and maturity models that we will continue to monitor going forward.

Security Training – OPM has implemented an IT security training program, but should perform a workforce assessment to identify any gaps in its IT security training needs.

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

Incident Response – OPM has made the greatest strides this fiscal year in the incident response domain. Based upon our audit work, OPM has successfully implemented all of the FISMA metrics at the level of "consistently implemented" or higher. As such, we are closing our FY 2016 recommendation related to the incident response program.

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

ABBREVIATIONS

ATO	**Authority to Operate**
Authorization	**Security Assessment and Authorization**
BIA	**Business Impact Analysis**
CDM	**Continuous Diagnostics and Mitigation**
CFC	**Combined Federal Campaign**
CISO	**Chief Information Security Officer**
CM	**Configuration Management**
DHS	**U.S. Department of Homeland Security**
FISMA	**Federal Information Security Modernization Act**
FY	**Fiscal Year**
HCDW	**Health Claims Data Warehouse**
ICAM	**Identity, Credential, and Access Management**
IG	**Inspector General**
ISCM	**Information Security Continuous Monitoring**
ISSO	**Information System Security Officer**
IT	**Information Technology**
NIST	**National Institute of Standards and Technology**
OCIO	**Office of the Chief Information Officer**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
PII	**Personally Identifiable Information**
PIV	**Personal Identity Verification**
POA&M	**Plan of Action and Milestones**
SDLC	**Systems Development Lifecycle**
SP	**Special Publication**
USAS	**USA Staffing System**

TABLE OF CONTENTS

I. BACKGROUND

On December 17, 2002, the President signed into law the E-Government Act (Public Law 107-347), which includes Title III, the Federal Information Security Management Act. This 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. On December 18, 2014, President Obama signed Public Law 113-283, the Federal Information Security Modernization Act (FISMA), which reiterates the need for an annual IG evaluation. In accordance with FISMA, we conducted an audit of 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 reemphasizes the Chief Information Officer's strategic agency-wide security responsibility. At the U.S. Office of Personnel Management (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) 2018 Inspector General FISMA Reporting Instructions. This document provides a consistent form 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 FY 2018 metrics also mark a continuation of the work that OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency undertook in FY 2015 and FY 2016 to move the IG assessments toward a maturity model approach. In previous years, the Council of the Inspectors General on Integrity and Efficiency, in partnership with OMB and DHS, transitioned two of the National Institute of Standards and Technology (NIST) Cybersecurity Framework function areas to maturity models, with other function areas utilizing maturity model indicators.

The FY 2018 IG FISMA Reporting Metrics completed this work by transitioning the remaining function areas to full maturity models. Our audit and reporting approaches were designed in accordance with DHS 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.

In addition, we evaluated the status of OPM's IT security governance structure and the agency's system Security Assessment and Authorization (Authorization) methodology, areas that have represented a material weakness in OPM's IT security program in prior FISMA audits. We also followed-up on outstanding recommendations from prior FISMA audits (see Appendix II), and performed audits focused on three of OPM's major information systems – the implementation of the Combined Federal Campaign (CFC), the USA Staffing System (USAS), and the Health Claims Data Warehouse (HCDW).

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 2018.

We reviewed OPM's general FISMA compliance efforts in the specific areas defined in DHS's guidance and the corresponding reporting instructions. We also performed information security audits on the CFC, USAS, and HCDW major information systems and the Authorization methodology. 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. This understanding of these systems' internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented. As appropriate, we conducted compliance tests using judgmental sampling 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 2018 Inspector General Federal Information Security Modernization Act Reporting Instructions;

- OPM Information Technology Security and Privacy Policy Handbook;

- OPM Information Technology Security FISMA Procedures;

- OPM Security Assessment and Authorization Guide;

- OPM Plan of Action and Milestones Standard Operating Procedures;

- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;

- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;

- OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive 12;

- P.L. 107-347, Title III, Federal Information Security Management Act of 2002;

- P.L. 113-283, Federal Information Security Modernization Act of 2014;

- NIST Special Publication (SP) 800-12, Revision 1, An Introduction to Computer Security: The NIST Handbook;

- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems;

- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;

- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;

- NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems;

- NIST SP 800-39, Managing Information Security Risk – Organization, Mission, and Information System View;

- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems;

- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;

- NIST SP 800-60, Volume 2, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories;

- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information;

- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems;

- Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems;

- Federal Cybersecurity Workforce Assessment Act of 2015;

- Federal Identity, Credential, and Access Management Roadmap Implementation Guidance;

- Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules; and

- Other criteria as appropriate.

The audit was performed by the Office of the Inspector General (OIG) at OPM, as established by the Inspector General Act of 1978, as amended. Our audit was conducted from April through September 2018 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

Management comments on the draft FISMA audit report

As we have noted many times in conversations with OPM and OCIO officials, the objective of our IT audit work is to identify control weaknesses in OPM's IT security program, from a policy, governance, and technical perspective, and recommend corrective action as needed. We share the OCIO's goal of achieving a mature IT security program that will adequately protect OPM's sensitive systems and data.

It is understandable that an organization's dedicated officials working hard to improve their operations would be disappointed with negative feedback. Even so, OPM's response to the draft FISMA audit report was unusually adversarial, challenged our authority to make recommendations in certain areas, and asserted that our work violated Government Auditing Standards.

Based on OPM's response to our draft FISMA audit report, and from follow-up meetings with senior OPM and OCIO officials, we understand that there is a concern that we have not fairly "credited" OPM for progress in its IT security program. There is no doubt that OPM has significantly improved its technical security posture in recent years by implementing two-factor authentication at the network level, data encryption and other data loss prevention tools, improved monitoring and incident response, and better procedures for updating software patches. OPM engineers designed a more secure, segmented network architecture and introduced client security to better control users accessing the network.

OPM's perimeter security controls have greatly improved since 2015, meaning that it would be more difficult for a malicious adversary to gain remote access to the network. Internal firewalls and network segmentation would limit a hacker's ability to traverse the network, escalate privileges, or steal sensitive data.

A common assumption in IT security, though, is that no matter how secure a network perimeter is, skilled adversaries will eventually compromise it, if it has not been already. For this reason, security controls at the system level are critical to an organization's overall security. At OPM, these controls need to be improved. In particular, only 6 of 54 OPM major systems require two-factor authentication, relying instead on unsecure user IDs and passwords for user authentication. In addition, monitoring and testing system security controls continues to be a challenge for OPM (see Section F).

Of greater concern is that security controls are perishable and rely on proper governance and management. This is an area in which OPM has historically struggled, and to some extent is a result of agency culture and the degree to which IT operations continue to be inappropriately decentralized. We have assessed IT security governance to be either a material weakness or a significant deficiency in OPM's internal control structure every year since 2008. This year we are again reporting a material weakness in OPM's IT security governance (see Section B) for several reasons, but primarily because of degraded compliance with critical FISMA metrics.

In our judgment, the cause of non-compliance is that OPM has not provided adequate resources to the OCIO to effectively manage the agency's IT operations and security (see section B for further discussion of this topic). Despite our recommendation in FY 2010 that OPM implement a centralized team of information system security officers dedicated to managing the IT security of OPM's major IT systems, the agency has still not developed a mature capability in this area. While part of the problem is one of resources, effective management of a skilled team of security experts is also needed. The result of this is an inadequate security assessment and authorization program, incomplete testing of system security controls and contingency plans, and lack of corrective action for identified weaknesses.

OPM's response to the draft FISMA audit report also questioned the IG's authority to recommend corrective action in these areas, stating that "the OIG's comments intrude on the broad discretion afforded to the agency by FISMA" (see Appendix III, page 2). OPM cites our comments on its "staffing decisions" as one instance of this intrusion. Another example given is our recommendation that OPM adopt an automated solution for tracking agency-wide risk. OPM asserts that since there is no requirement for automated tools, our recommendation "intrudes on OPM's discretion to identify the right tools for its unique needs."

Setting aside for the moment the merit of our recommendations, OPM's comments reveal a misunderstanding of the role of a Federal Office of Inspector General with respect to the agency it oversees. The Inspector General Act of 1978, as amended, created independent and objective units "to conduct audits … relating to the programs and operations" of the agency "to … recommend policies … to promote economy, efficiency, and effectiveness in the administration of … such programs and operations; and to provide a means for keeping the head of the establishment and the Congress fully and currently informed about problems and deficiencies related to the administration of such programs and operations and the necessity for and the progress of corrective action … .".

We do not agree that making recommendations to promote economy and efficiency in the agency's programs and operations related to the allocation of resources or the use of specific tools "intrudes" on the agency's discretion. The idea that certain areas of a Federal department or agency would be "out of bounds" for a Federal Office of Inspector General to review and recommend corrective action runs counter to the spirit and letter of the IG Act and its various amendments.

OPM also asserts in its response to our draft FISMA audit report, without specifics, that "a number of the conclusions reached by the OIG in this report appear to be unsubstantiated or reflect a subjective opinion." On the contrary, our audit was conducted in strict compliance with Generally Accepted Government Auditing Standards, also known as the Yellow Book, which provides a "framework for conducting high-quality audits with competence, integrity, objectivity, and independence."

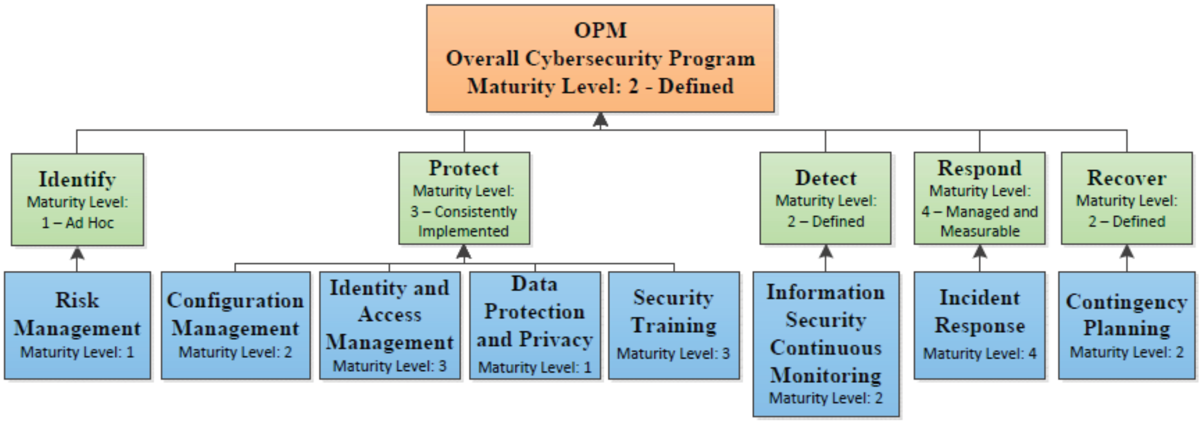
Federal Office of Inspector General auditors are required to adhere to Yellow Book standards. Yellow Book Section 6.03 defines the auditor's responsibility to obtain reasonable assurance that evidence is "sufficient and appropriate to support the auditors' findings and conclusions …." Yellow Book Section 3.61 states that "Auditors must use professional judgment in planning and performing audits and in reporting the results."

Our findings and conclusions are not "unsubstantiated," but are supported by relevant and sufficient evidence gathered during the audit. In addition, to the extent that the results of our audit are "subjective," they are based on our professional judgment, competence, and experience. Further, our ratings for the maturity model metrics (discussed in summary below, and in detail starting on page 20) were informed by guidance provided by the Council of the Inspectors General on Integrity and Efficiency, the U.S. Office of Management and Budget, and the U.S. Department of Homeland Security.

We would also like to note that numerous times in the OCIO's response to the draft FISMA audit report, the OCIO indicated it did not have a clear understanding of what evidence is needed to address an open recommendation. The OCIO also indicated in several instances that they had previously provided the necessary documentation to address a recommendation. Prior to the beginning of fieldwork, the OIG met with the OCIO to review the status of open recommendations and ways to demonstrate corrective action has been taken. In addition, throughout the duration of the audit status meetings were held to discuss information requests made by the OIG that were still outstanding. Thus, there were multiple opportunities for the OCIO to provide, or indicate that they had already provided, documentation to the OIG. Finally, the OCIO does not regularly follow OPM's established processes for managing the resolution of audit recommendations through the agency's Internal Oversight and Compliance office. These processes involve establishing and executing corrective action plans, and tracking the status of results, and is overseen by OPM management.

Maturity Model Assessment

The FY 2018 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 are mapped to eight "domains" that fall under each function area. 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 is rated on a maturity level of 1 to 5. The overall maturity of OPM's cybersecurity program is outlined in the chart below: (detailed results by metric can be found in Appendix I):

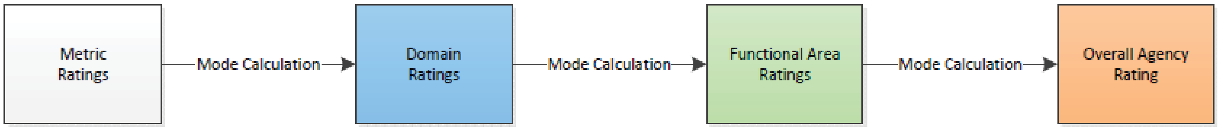


The following table outlines the description of each maturity level rating, as defined by the FY 2018 IG FISMA Reporting Metrics:

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. Similarly, the mode from the domain ratings is used to assign the function area rating. The overall agency rating is calculated using the same methodology.



The remaining sections of this report provide the detailed results of our audit. Most notably, since the data breach in 2015, OPM has made significant strides to implement an incident response program that is “managed and measurable” (see Section J). However, Information Security Governance and Security Assessment and Authorizations (Sections B and C, respectively) do not directly map to the FY 2018 IG FISMA Reporting Metrics but warrant discussion in this report. Sections D through K 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. INFORMATION SECURITY GOVERNANCE

Information security governance is the foundation of a successful information security program. This includes a variety of activities, challenges, and requirements, but is primarily focused on identifying key roles and responsibilities and managing information security policy development, oversight, and ongoing monitoring activities.

OPM’s information security governance program has been a longstanding concern. We have assessed it to be a material weakness or a significant deficiency in OPM’s internal control structure every year since FY 2007. This year, we again consider deficiencies in the agency’s information security governance program to be a material weakness in the agency’s IT security internal control structure. OPM has made some recent progress updating and maintaining policy documents, implementing standard procedures, and centralizing its cybersecurity program under a Chief Information Security Officer (CISO) supported by a team of Information System Security Officers (ISSO).

However, as noted in Section A, OPM's cybersecurity program has not reached the level of maturity that would facilitate the consistent application of FISMA requirements. For example, OPM has not been able to complete the annual requirement to independently test the security controls and contingency plans of all of its major IT systems since 2008. What this means is that, in some cases, mission-critical IT systems with highly sensitive data may have inadequate security controls or may not be recovered in the event of a disaster.

OPM's security assessment and authorization process (SA&A) is similarly inadequate. While some progress was made during the agency's 2016 'sprint' there has been a relapse since then (see Section C for details). Even if OPM's SA&A process was well managed, it would still be considered an outdated technique for managing IT risk. NIST SP 800-137, published in September 2011, introduced the risk management framework and the concept of continuous monitoring of vulnerabilities and threats to information systems to replace the triennial SA&A process. Despite some effort, OPM has not made sufficient progress in adopting a mature continuous monitoring program (see Section I on ISCM).

Another shortcoming in the OCIO's overall governance program is its inability to manage and implement corrective action for control weaknesses identified through audits or other types of reviews. OPM has not implemented corrective action for any of the 39 recommendations in our FY 2017 FISMA report, and has only closed 5 of the 26 recommendations in the FY 2016 FISMA audit report. Further, the OCIO's process for managing plans of action and milestones for correcting IT security control weaknesses is inadequate (see Section D).

The OCIO does not follow OPM's established processes for managing the resolution of audit recommendations through the agency's Internal Oversight and Compliance office. These processes involve establishing and executing corrective action plans, and tracking the status of results.

The OCIO has made progress implementing corrective action on recommendations made in four GAO audit reports issued between 2016 and 2018. As of September 2018, OPM had implemented 51 of 80 GAO information security program and control recommendations. While on the surface this is impressive, it should be noted that 46 of the closed recommendations were specifically associated with two high-impact systems, and 21 of these 46 recommendations were closed, not because the OCIO had actually implemented corrective action, but because one of the systems had been decommissioned.

The OCIO should be commended for its progress in implementing corrective action on the GAO audit recommendations. But this corrective action was primarily focused on two systems and not on strategic, enterprise-level controls. There is no evidence that the OCIO has improved its overall program for managing corrective action of identified security control weaknesses.

However, the OCIO did award a contract to a vendor in May 2018 to help establish an enterprise program management office (EPMO) with three objectives:

1. Improve overall IT governance;

2. Establish a technical enterprise architecture; and

3. Implement improved procedures for managing corrective action.

While this is positive, it remains to be seen whether this project leads to lasting, long-term improvement in OPM's overall IT security program. The contract has one base year, with options for two additional years, but the contract was financed with IT modernization funds and the EPMO is not staffed with fulltime Federal employees. There does not appear to be a plan for long-term funding and staffing.

Another ongoing issue emerged in FY 2018 regarding "shadow IT" systems, applications, and data. The OCIO discovered at least 30 systems operating in its production environment without defined boundaries, required security documentation, or an Authority to Operate. The OCIO's initiative to bring clarity to the IT environment, and its discovery of these undocumented systems, reflects positively on its ongoing efforts to enhance security controls and improve documentation.

But this is a larger problem rooted in OPM's history and culture, and further evidence that the agency's IT security governance program needs improvement. OPM's program offices in many cases avoid involving the OCIO when acquiring or changing IT systems that support their business operations. While some progress has been made to centralize IT under the OCIO, OPM's leadership has not fully adopted statutory requirements regarding the authority of Federal CIOs. OPM's program offices often avoid centralized IT security requirements and processes through outsourcing system development, modification, or hosting services without OCIO involvement.

Good governance requires centralized authority and control over all IT systems development and operation in an agency. Without this, there is the potential for security vulnerabilities and poor IT project management as individuals outside of the OCIO may not be fully versed in all security requirements or best practices. Additionally, we have observed instances where OCIO involvement early in the process would have avoided costly contract modifications to ensure system compliance with security requirements.

All of these examples discussed above are symptoms of the underlying issues at OPM: there are inadequate resources to fully support OPM's IT environment, and the agency has not historically viewed the OCIO as a strategic partner on par with other program offices. Throughout this audit, and in many other situations, OCIO officials expressed to us that inadequate resources are the primary reason for the lack of progress in making the structural reforms needed to achieve strong IT security governance.

In July 2017, OPM's prior CIO prepared a document laying out a framework for strengthening OCIO operations. In the document, entitled "CIO Value to OPM for Director, OPM," the prior CIO also discussed the budget and cultural limitations that adversely impacted his efforts to implement this framework. OPM's prior Deputy CIO, who recently departed, provided a copy of this document to our office, and verbally emphasized many of the points presented in the paper.

As discussed in Section (A) of the "CIO Value" document, after the OPM data breaches in 2014 and 2015, OPM's effort to improve its technical IT security controls exhausted funds available to maintain base IT operations in FY 2016. A supplemental appropriation of $37 million for IT modernization requested in FY 2017 never materialized, and OPM's FY 2017 budget was not approved until May 2017. As a result, OPM cut back on planned modernization work and applied a hiring freeze, forcing the OCIO to reduce its operational activities.

OPM's budget process involves funding from several sources, including trust funds, revolving funds, and a salaries and expenses fund. There is also a "common services" allocation from OPM's OCFO to fund support services such as IT, procurement, financial services, and facilities. The OCFO develops a formula to collect the "common services" from each program office, and then distributes those funds to the support offices. As discussed in our *Audit of the U.S. Office of Personnel Management Common Services* (OIG Report No. 4A-CF-00-16-055, March 29, 2018), this process is not clearly defined or transparent.

The OPM-administered trust and revolving fund monies allocated to the OCIO must be used for the IT systems that support those activities. For core information technology services, including security controls, the OCIO is completely reliant on the salaries and expenses fund, and its common services allocation from the OCFO. In the "CIO Value" document, OPM's prior CIO discussed how this arrangement has resulted in "significant funding challenges" facing the

OCIO, which he believed demonstrated the "lack of support and transparency for the OCIO organization over the years."

In FY 2016, OPM's Congressional Budget Justification included $21 million for OPM to "implement **and sustain** agency network upgrades and security software maintenance … This updated network must be maintained over time to ensure that OPM's system does not revert to antiquity and insecurity." (emphasis added). This funding was included in the OCIO's FY 2016 budget but was subsequently absorbed into OPM's core budget in FY 2017, resulting in a decrease in the OCIO's operating funds of almost $10 million. Because this funding was no longer available to support ongoing maintenance costs associated with updated security tools, the OCIO was forced to reduce spending that could have otherwise been used for fundamental reforms. The prior CIO noted in the "CIO Value" document that only one-third of OPM's overall spending on IT was controlled by the OCIO.

Strengthening financial performance was one of the prior CIO's top five priorities through FY 2020. The focus areas in this priority were improved transparency of overall IT spending in the agency and replacing the common services budget process with a cost accounting model to better identify the true costs of OCIO services to agency components.

The prior CIO expressed in the "CIO Value" document that "The OCIO has not been seen as an important, innovative partner in support of all OPM business lines, one that brings value or technological capabilities required to achieve the most effective and efficient mission delivery." His suggested framework for improving the OCIO's operations was based, in part, on transparency in costs, centralized authority for IT procurement within the OCIO, and including the OCIO in the strategic-level decision making process.

This "CIO Value" document is only the viewpoint of two prior senior OCIO officials, although we consider both to be highly respected and experienced. Based on our experience and observations over a number of years, and recent audit work regarding OPM's Federal Information Technology Acquisition Reform Act compliance, we agree with the overall position that the OCIO does not have adequate resources to effectively manage IT operations and security, and that the agency has not historically valued the proper role of a Federal CIO.

This may be why there has also been an unusually high turnover in key OCIO senior positions at OPM. There have been six CIOs in the last three years and the deputy CIO recently left the agency. The prior CISO moved on to another position, and the acting CISO is also a senior official responsible for running the agency's infrastructure – a clear separation of duties problem.

As a result, OPM continues to struggle to implement a mature and consistent overall IT security program. Progress in one area usually comes at the expense of regression in another.

There is insufficient staff to maintain basic operational or security requirements. Specifically, in FY 2018 OPM was downgraded in FISMA metrics related to risk management (see Section D), and received low maturity level scores for continuous monitoring (see Section I), and contingency planning (see Section K).

Recommendation 1 (Rolled forward from 2016)

Note: The recommendation in the draft FISMA audit report was focused on recruitment of information system security officers. Based on information received after the draft report was issued, we modified this recommendation in the final audit report to address the more strategic level discussion of resource issues affecting the OCIO.

OPM does not have the appropriate resources in place to manage its cybersecurity program.

We recommend that the OPM Director ensure that the OCIO has sufficient resources to adequately operate, secure, and modernize agency IT systems.

We also recommend that the agency hire a sufficient number of Information System Security Officers (ISSOs) to adequately support all of the agency's major information systems.

OPM Response:

"We concur with the recommendation. The OPM OCIO conducted an analysis on the funding requirements for ISSO positions and understands where the gaps are. OPM is actively recruiting for these positions, having extended two offers at the end of September and continuing with interviews into early October."

OIG Comment:

As part of the audit resolution process, we recommend that the OCIO provide OPM's Internal Oversight and Compliance office with evidence that this recommendation has been implemented. This statement applies to all subsequent recommendations in this audit report that the OCIO agrees to implement.

Recommendation 2

We recommend that OPM ensure that the OCIO's senior leadership vacancies are filled and that there is a proper separation of duties for assigned roles and responsibilities.

OPM Response:

"We concur with the recommendation. OPM understands the importance of having the individual in the role of the Chief Information Security Officer have information security as his or her primary duties, and will assign an individual to this role in Fiscal Year (FY) 2019."

C. SECURITY ASSESSMENT AND AUTHORIZATION

Authorization is a process that includes both a comprehensive assessment that evaluates whether a system's security controls are meeting its security requirements, and an attestation that the system risks are at an acceptable level. Both OPM policy and NIST guidance require each system to have a current Authorization.[1]

Like OPM's IT security governance program, we have reported either a material weakness or a significant deficiency in OPM's Authorization process every year since FY 2014 because of incomplete, inconsistent, and sub-par work products. OPM implemented new policies and procedures to standardize its processes, but was not able to maintain a current Authorization for all major systems in its system inventory.

After significant effort from OPM in FY 2017, the agency had established valid Authorizations for its major information systems, including the critical general support systems. The OCIO had also successfully addressed some of the weaknesses that our audits identified, but there were still widespread issues primarily related to documentation inconsistencies and incomplete or inadequate independent testing of the systems' security controls.

As part of the FY 2018 audit, we requested Authorization documentation supporting 23 of OPM's 54 major systems. During the audit, the OCIO only provided a current Authorization for 18 of the 23 systems under review. In addition, we found that many of the 18 Authorization packages for these systems were not in compliance with NIST requirements. They either were missing critical elements or were of such poor quality that it was unclear that an effective risk

[1] The OCIO has continued its efforts to implement a comprehensive continuous monitoring program that will eventually replace the need for periodic system Authorizations. However, OPM's continuous monitoring program has not reached the point of maturity where it can effectively replace the Authorization program (see Section I, Information Security Continuous Monitoring).

decision was possible. Just before the draft FISMA audit report was issued, the OCIO provided three additional Authorization letters (see OIG Comment for Recommendation 3 for additional details).

Based on the information available at the time our draft FISMA audit report was issued, we determined that the inadequate Authorization process represented a material weakness in the agency's IT security internal control structure. Specifically, the documentation that the OCIO provided indicated that there were five systems operating in the production environment without a valid Authority to Operate (ATO). In addition, many of the other production systems had ATOs based on flawed Authorization packages.

However, based on the information we received after the draft report was issued, we believe that the current control weaknesses are less severe than a material weakness, but are still a significant deficiency in IT security controls. While there now appears to be a valid Authorization in place for almost every major IT system in the agency's system inventory (see the OIG Comment for Recommendation 3 for additional details), the quality of the work and supporting documentation is questionable.

In addition, we noted that in some cases, the OCIO issued short-term or interim ATOs in violation of OMB guidance. OMB does not recognize interim ATOs for at least two reasons. First, security should be included in the budgeting life cycle of all IT systems. The lack of planning or budget is not a valid reason to extend existing ATOs, and the existence of open weaknesses identified during the Authorization process is not a reason to issue a short-term ATO. The second reason is to ensure consistency and quality in Government-wide reporting.

Furthermore, the newly identified "shadow IT" systems, applications, and data (discussed in Section A) have not been evaluated for inclusion on the major system inventory. It is likely that at least some of them will be considered major IT systems that must be subject to the Security Assessment and Authorization process. There is a high risk that these undocumented and unauthorized systems have control weaknesses that could compromise the agency's overall IT security program.

Recommendation 3 (Rolled forward from 2014)

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

OPM Response:

"We do not concur with the recommendation based on the conditions of the recommendation. While OPM agrees with the premise that all active systems in the inventory must have a complete and current authorization, it does not agree with the OIG's conclusion that discovery of assets means that the system inventory and related authorizations are not complete. As referenced by the OIG, significant efforts have been taken by OPM to identify hardware and software assets on its network, including better detection of system boundaries, showing that actions have already been taken that are consistent with past OIG recommendations in this area and that achieve the goal of those recommendation. Issuance of this recommendation along with the supporting language in the report suggests that OPM's posture has worsened, when in fact the work being done in this area clearly shows that OPM has been making strides in the maturity of these programs. Every active system within the inventory has a complete and current authorization and OPM provided to OIG the authorization letters for each system within its system inventory during this annual audit. If systems are identified as a part of OPM' s continuous monitoring activities, they will be added to the inventory after completing an assessment and authorization, as appropriate, for that system."

OIG Comment:

After issuance of the draft audit report we were provided additional Authorizations for three systems on OPM's inventory. However, there are 2 systems of the 23 reviewed for which we have not received a current Authorization. Both of these systems are implemented on platforms supported by cloud service providers. OPM policy requires both that the platform be FedRAMP certified and that the agency-specific system be appropriately authorized. We received documentation from the FedRAMP certification for both platforms; however we have not received the agency's Authorizations for the specific systems.

Apart from these two systems it is more than likely that there are missing systems on OPM's inventory. During our discussions about recently discovered systems, OCIO officials indicated a number of these systems would need to be added to the major system inventory. We do agree with OPM that the progress made with finding previously unknown assets is positive. However, we have not seen any evidence that shows these systems have been assessed to determine whether they are major systems, which would necessitate inclusion on OPM's major system inventory and require Authorizations.

Recommendation 4 (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. The agency has taken, and will continue to take, OIG's recommendation under advisement and agrees that system owners provide support to the business processes of the agency. However, performance metric adjustments would need input and guidance from the Human Capital Office. Apart from changes to performance standards, OPM will continue to identify appropriate ways to work with system owners to help ensure FISMA compliance. For instance, recently issued cybersecurity policies set forth expectations and requirements for system owners, consistent with NIST 800 Series guidance."

OIG Comment:

The cybersecurity policies that set forth expectations for system owners referenced by OPM were not provided to us during the course of this audit. Historically, OPM has had difficulty keeping systems compliant with FISMA requirements. Although OPM disagrees with this recommendation, the OIG stands by its position that the best approach to ensure that systems are compliant with FISMA requirements is to include these in the performance standards for system owners. Incomplete and inadequate SA&A documentation has been an ongoing issue for OPM and this approach would help ensure the SA&A process is followed routinely as required by FISMA.

We agree with OPM that performance metric adjustments would most likely need input from the Human Capital Office. Its involvement would be an effective step in developing a corrective action plan to address this recommendation.

D. RISK MANAGEMENT

Risk management controls are the tools, policies, and procedures that enable an organization to understand and control risks associated with its IT infrastructure and services. These controls should be implemented throughout the agency and used to support making risk-based decisions with limited resources. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Risk Management domain is "1 – Ad-hoc."**

Metric 1 – Inventory of Major Systems and System Interconnections

FY 2018 Maturity Level: 1 – Ad-hoc. OPM policy requires that the agency keep a major system inventory, to include system interconnections.[2] While the agency has established a central repository for its system inventory, agency procedures require that system boundaries be defined before the system can be properly classified. At that point the system can be added to the system inventory and undergo the Authorization process. OPM has historically struggled to fully define its existing system boundaries as management of OPM systems has been decentralized. As mentioned in Section C, OPM's OCIO has taken steps to centralize the management of IT and identify undocumented systems in the agency's environment. As a byproduct of this effort, OPM continues to discover existing systems, interconnections, and data that are not properly classified and inventoried in its environment.

The current policy and procedures for defining system boundaries and classifying systems does not appear to contain a sufficient level of detail to be consistently enforced. As a result, there are systems in the production environment currently in a state of limbo without a defined boundary, classification, or Authorization. This issue also relates to both Metric 2 and Metric 3 for risk management. If the OPM hardware and software inventories were properly correlated to the boundaries of the systems in the environment, there would be less risk of discovering improperly classified systems.

NIST SP 800-53, Revision 4, requires that an organization "Develops and maintains an inventory of its information systems." Furthermore, NIST requires an organization "Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated . . ." and that each connection should be authorized, and then regularly reviewed and updated.

Failure to document and approve all systems and system interconnections increases the risk that information systems will improperly contain, share, or fail to protect sensitive information.

Recommendation 5

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

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

OPM Response:

"We do not concur with the recommendation. OPM believes the OIG has provided no basis for determining that the current policy and procedures for defining system boundaries and classifying systems do not contain a sufficient level of detail to be consistently enforced. The OIG simply states that "[t]he current policy and procedures for defining system boundaries and classifying systems does not appear to contain a sufficient level of detail to be consistently enforced." (emphasis added). The agency considers its policy, which is based on NIST guidance and recommendations, to be sufficient and without need of further improvement. Nonetheless, although it is our view that we have fulfilled the requirements of this recommendation, OPM asks the OIG to clarify their rationale on this recommendation."

OIG Comment:

Regarding the agency's statement in their response, "***The agency considers its policy, which is based on NIST guidance and recommendations, to be sufficient and without need of further improvement",*** there are three OPM documents we reviewed (the security policy, the procedure guide, and the documentation template) that provide guidance for system documentation. The most recent of the three documents reviewed is more than two years old. There was no more than a sentence or two describing what to include in a system's authorization boundary in each letter. As stated in Metric 1, OPM continues to discover systems, applications, and data outside of current system boundaries. The guidance for classifying systems is slightly more detailed. However, there have been discussions with the OCIO about systems that have changed or might change classifications on what appears to be individual preference or opinion rather than defined criteria. Without clearly defined guidance for defining and classifying systems, OPM's issues with its major inventory and system authorizations will most likely continue.

Recommendation 6 (Rolled forward from 2014)

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

OPM Response:

"We concur with the recommendation. Continued updates to centralized tracking, including those that have been released in September, 2018, will improve overall management of the Interconnection Security Agreements (ISAs)."

Recommendation 7 (Rolled forward from 2014)

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

OPM Response:

"We concur with the recommendation. Continued updates to centralized tracking, including those that have been released in September, 2018, will improve overall management Memorandum of Understandings (MOUs)."

Metric 2 – Hardware Inventory

FY 2018 Maturity Level: 2 – Defined. OPM uses a software tool to maintain a centralized inventory of its hardware assets. The inventory contains details of the hardware such as type, model, serial number, location, and status. OPM's hardware inventory includes many of the required elements, but it does not contain information that associates hardware components to the major system(s) that they support.

NIST SP 800-53, Revision 4, states that organizations with centralized inventories must "ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association and information system owner)."
Failure to 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 8 (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 relies on support from the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program to support the implementation of these requirements. OPM has been at the forefront of working with DHS throughout the lifecycle of the CDM program and will maintain this partnership as CDM continues to evolve. The recommendation here underscores efforts across the Federal government and is not unique to OPM."

Metric 3 – Software Inventory

FY 2018 Maturity Level: 1 – Ad-hoc. In FY 2017, OPM provided the OIG with a list of software in its environment. While the list was incomplete and missing information, it was an adequate start of a centralized inventory. In response to our FY 2017 FISMA audit report, OPM indicated that it was working towards an inventory that correlated the software list with the centralized system inventory. However, OPM has changed its position this year and no longer has a centralized software inventory. Instead, OPM now tracks software information at the system level.

NIST SP 800-53, Revision 4, states that organizations with centralized inventories must "ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association and information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location."

Failure to maintain a centralized software inventory increases the risk that the agency will not fully understand the information assets in its environment or maintain a complete major system inventory. This increases the agency's susceptibility to unassessed risks and undetected vulnerabilities because major systems are not undergoing the Authorization process. Another disadvantage of decentralized software management is likely excess expense from the lost opportunity to bundle software licensing or fully achieve volume discounts that could be available at the agency-wide level.

Recommendation 9

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

OPM Response:

"We do not concur with the recommendation. While we concur with the general premise of having policies and procedures related to a centralized software inventory, OPM notes that it already has appropriate policies and procedures in place. The OIG states that, 'OPM has changed its policy and no longer has a centralized software inventory…' This statement is not correct. OPM issued a Secure Asset Management Policy in January 2018 to reinforce existing asset management requirements and define requirements for management of hardware and

software assets. The implementation of a centralized repository for the inventory of these assets is explicitly required by the policy. OPM has also issued an Information Security Continuous Monitoring Strategy, referenced by the OIG in Section I.

Further, the OIG report references supplemental guidance from the NIST 800-53, Rev. 4, CM-8 security control in the text related to this recommendation. However, NIST guidance affords agencies significant latitude to determine whether to implement a centralized inventory, and implementation of a centralized inventory is not part of a baseline control per NIST guidance. Therefore, in essence, the OIG's conclusion that there is a deficiency is based on a determination that OPM has not implemented controls that exceed the baseline. Such a conclusion intrudes on matters within the agency's discretion."

OIG Comment:

The information conveyed to us during our interviews, status meetings, and the exit conference with OCIO staff and management was that a centralized software inventory would not be feasible given the current prevalence of shadow IT systems throughout the agency. The Secure Asset Management Policy was not provided to us during the course of our audit fieldwork.

The OIG is not limited to NIST guidance when identifying criteria for developing audit programs and making recommendations. Industry best practices are also considered when making recommendations. A centralized software inventory management approach would provide the greatest control over software installed throughout the agency. Additionally, this ensures cost savings by reducing redundancy and facilitating volume discounts during the procurement process.

Recommendation 10 (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. OPM completed the definitions for standard data elements for an inventory of software assets and licenses at the ·end of August 2018. The standard data elements are provided along with this response. OPM continues to work with DHS on the implementation of the CDM program and will adopt these data elements within its current software asset management capabilities."

Metric 4 – System Security Categorization

FY 2018 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 2018 Maturity Level: 1 – Ad-hoc. OPM's OCIO has defined policies for assessing and reporting IT-related risks. OPM's Risk Management Council serves as the primary risk executive function and is responsible for the agency-wide risk management program. The council meets regularly and has defined a risk profile for OPM, but has not yet established an overall risk strategy for the agency.

OPM created a Risk Management Council to serve as the risk executive function and develop the agency-wide risk management approach.

An effective risk management strategy provides the guidance for understanding, tracking, and addressing risks, as well as making risk-based decisions for agency systems and resources. Without an approved risk management strategy, the agency will not be able to effectively create and define consistent agency-wide risk management policies and procedures.

NIST SP 800-39 requires that a risk management strategy include "the risk tolerance for the organization, acceptable risk assessment methodologies, risk response strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time." It also states that the strategy must "[make] explicit the specific assumptions, constraints, risk tolerances, and priorities/trade-offs used within organizations for making investment and operational decisions."

Without a risk management strategy, there is an increased likelihood that the agency will not have or consider the proper risk information when making investment, security, and operational decisions.

Recommendation 11 (Rolled forward from 2017)

We recommend that OPM define and communicate a risk management strategy based on the requirements outlined in NIST SP 800-39.

OPM Response:

"We concur with the recommendation. OPM published a Cybersecurity Risk Management Strategy based on the requirements in NIST SP800-39 in September 2018. The Cybersecurity Risk Management Strategy can be provided upon request."

Metric 6 – Information Security Architecture

FY 2018 Maturity Level: 1 – Ad-hoc. OMB's Federal Enterprise Architecture Guidance states that an enterprise architecture "describes the current and future state of the agency, and lays out a plan for transitioning from the current state to the desired future state."

In FY 2017, we reported that OPM's enterprise architecture had not been updated since 2008, and does not support the necessary integration of an information security architecture. OPM acknowledged this and incorporated remedial efforts as a part of OPM's FY 2017 and FY 2018 IT Modernization Spending Plan. (For more information on these spending plans see Management Advisory Nos. 4A-CI-00-18-022 & 4A-CI-00-18-044, dated February 15, 2018, and June 20, 2018, respectively). A contract was awarded and efforts are underway to begin developing an enterprise architecture. Despite projected completion dates well into FY 2019, we are hopeful that OPM will be able to properly integrate the necessary information security architecture as a part of this process.

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 that "The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes."

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

Recommendation 12 (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. As stated in the report, a contract was awarded and activities are in progress to develop the enterprise architecture. Despite projected completion dates well into FY 19, we expect that OPM will properly integrate the necessary information security architecture as a part of this process."

Metric 7 – Risk Management Roles, Responsibilities, and Resources

FY 2018 Maturity Level: 2 – Defined. OPM has defined the necessary roles and responsibilities of stakeholders in its risk management program. This includes outlining the role of the Risk Management Council, and defining the responsibilities of information system owners, information security staff, and authorizing officials. The Risk Management Council has created an agency risk profile, but is not yet fulfilling all of the responsibilities of the risk executive function required by NIST. Specifically, OPM does not have a documented risk strategy. In addition, the resource limitations noted in Section B, Information Security Governance, also negatively impact the risk management program, since the CISO organization plays a key role in tracking IT risks at the system level.
NIST SP 800-39 lists the required responsibilities of the risk executive function, including to "Develop and implement an organization-wide risk management strategy that guides and informs organizational risk decisions . . ." and to "Provide oversight for the risk management activities carried out by organizations to ensure consistent and effective risk-based decisions . . . ."

Without all of the elements of the risk executive function in place, there is an increased likelihood that OPM's risk management program will not fully identify agency risks or make effective risk-based decisions for its resources and programs.

Recommendation 13 (Rolled forward from 2011)

We recommend that OPM continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, Section 2.3.2 Risk Executive (Function).

OPM Response:

"We partially concur with the recommendation. As described under Recommendation 11, OPM published a Cybersecurity Risk Management Strategy based on the requirements in NIST SP 800-39 in September 2018. OPM also drafted an Enterprise Risk Management Policy, Enterprise Risk Management Strategy, and an updated charter for the Risk Management Council. OPM expects to finalize and operationalize these documents early in

the first quarter of FY 19. OPM does not concur that the resource limitations described in Section B of the report will impact OPM's ability to develop its Risk Executive Function since those resource limitations are not a part of that function."

<u>OIG Comment:</u>

We recognize that the Risk Executive Function has been established and stakeholders have been defined and communicated across the organization, including the CISO organization. However, stakeholders must have adequate resources (i.e., people, processes, and technology) to effectively implement risk management activities. As noted in other areas throughout this report, the lack of resources in the CISO organization affects the execution of risk management activities, such as system level risk assessments, and Plans of Action and Milestones. The development of the Risk Executive Function could benefit from CISO input as it shoulders a significant responsibility.

Metric 8 – Plan of Action and Milestones

<u>FY 2018 Maturity Level: 2 – Defined.</u> The Plan of Action and Milestones (POA&M) is a tool used to track known weaknesses in information system controls and the corresponding remediation efforts. Previous FISMA audits identified serious issues with the OPM POA&M process, primarily related to system owners not meeting the self-assigned scheduled completion dates for remediating weaknesses. As a part of the IT Modernization Spending Plan discussed in Metric 6, OPM awarded a contract to develop a more effective process for implementing corrective action related to outstanding POA&Ms and audit recommendations. This effort is underway in connection with the contract to establish an Enterprise Project Management Office (EPMO) at OPM.

While the additional funding has allowed OPM to begin the process of establishing an EPMO, the longstanding lack of adequate security resources (See Section B, Information Security Governance) continues to impact OPM's ability to effectively manage its POA&Ms. POA&Ms are required to contain information (e.g., POA&M status, remediation milestones, and planned completion dates) necessary to allow OPM officials to monitor progress of remediation efforts.

However, as of August 1, 2018, over 81 percent of POA&Ms were more than 30 days overdue, and over 68 percent were more than 120 days overdue. The process of tracking, updating, and closing POA&Ms is key to understanding the changing level of risk that a system faces and how that system affects the risks of the agency. Without up-to-date POA&M information the agency cannot make effective risk-based decisions and efficiently allocate resources to address risks.

Over 68 percent of POA&Ms are more than 120 days overdue.

As discussed in Section B, we continue to believe that OPM's failure to meet long-standing FISMA metrics (such as the ones in this section related to POA&Ms) is indicative of a material weakness in the agency's information security governance structure.

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

Recommendation 14 (Rolled forward from 2016)

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

OPM Response:

"We concur with the recommendation. The OCIO will use several processes to remediate this recommendation, including the new Enterprise Project Management Office (PMO), centralized POA&M management tool updates to streamline management of the POA&Ms, and quarterly performance management of POA&M processes."

Recommendation 15 (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. The OCIO will utilize several processes to remediate this recommendation, including the new EPMO, centralized POA&M management tool updates to streamline management of the POA&Ms, and quarterly performance management of POA&M processes."

Metric 9 – System Level Risk Assessments

FY 2018 Maturity Level: 2 – Defined. OPM has defined the policies and procedures for conducting risk assessments for individual information systems. OPM policy requires that each system be routinely assessed for risk as part of the Authorization process. Of the 23 system Authorization packages requested this fiscal year, complete risk assessments were not provided for 11, and widespread issues were noted with the security controls testing and/or the corresponding risk assessment. We found instances where not all of the applicable security controls were independently tested and instances where not all of the identified control weaknesses were included in the system risk assessments. Controls testing and risk assessments are a key part of the Authorization process, and the problems we found indicate that Authorizing Officials may not have all of the necessary risk information when granting an Authorization.

OPM policy requires, "All controls selected by the system . . . are assessed" and 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.

Recommendation 16 (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 this recommendation. Supported by agency leadership, the OCIO has committed to providing the resources and staffing to properly enforce compliance through ISSOs and the development of an independent assessment team of contractors. The independent assessment team has begun efforts to conduct risk assessments in a consistent manner."

Metric 10 – Risk Communication

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

Metric 11 – Contracting Clauses

FY 2018 Maturity Level: 3 – Consistently Implemented. OPM policy mandates the use of specific contracting language and service level agreements to ensure contractors meet both Federal and OPM standards. This language includes information privacy and security requirements, such as protection, detection, and reporting of information. This ensures that contractor systems and services are implementing required controls, and that OPM receives the information it needs to monitor and assess any risks. For both internal and external systems, OPM uses the same process to evaluate that controls are working properly and effectively to reduce risk.

Metric 12 – Centralized Enterprise-wide Risk Tool

FY 2018 Maturity Level: 1 – Ad-hoc. OPM does not have a centralized system or tool to view enterprise-wide risk information. The Risk Management Council has the responsibility of understanding and determining risk at the agency level, but this will be a monumental task and highly inefficient without centralized storage of agency-wide risk information. OPM has begun the preliminary effort to define the system requirements by documenting high-level system mandates (i.e., the Federal and agency requirements for security and processing standards). However, more work is still needed to define the system-level business and technical requirements necessary prior to any system development or acquisition to ensure the needs of the agency are met.

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

- "Manage threat and vulnerability information with regard to organizational information systems and the environments in which the systems operate";
- "Establish organization-wide forums to consider all types and sources of risk (including aggregated risk)";
- "Determine organizational risk based on the aggregated risk from the operation and use of information systems and the respective environments of operation"; and
- "Develop a greater understanding of risk with regard to the strategic view of organizations and their integrated operations . . . ."

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

Recommendation 17 (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 partially concur with the recommendation. OPM recognizes the need for tracking risks to OPM and OPM systems as defined in the OPM Risk Management Strategy; however, no federal requirements define the requirement for an automated centralized tool for tracking such risks. Additionally, OPM believes this recommendation may intrude on its discretion to allocate and manage resources in this area. Nonetheless, OPM exercised its broad discretion under FISMA to develop requirements for an automated enterprise-wide solution and will continue to leverage appropriate tools to document and manage risk related to OPM IT systems."

OIG Comment:

Metric 12 in the FY 2018 Inspector General FISMA Reporting Metrics specifically addresses the extent to which agencies utilize technology for tracking enterprise-wide risk. In order for OPM to move to the defined maturity level it must identify its requirements for an automated solution that provides a centralized, enterprise-wide view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards.

We agree that OPM should have broad discretion in identifying an automated enterprise-wide solution that meets the agency's specific needs. However, our recommendation for OPM to develop requirements and implement a solution is consistent with the Maturity Level Descriptions. As previously stated, we do not agree that making recommendations to promote economy and efficiency in the agency's programs and operations related to the allocation of resources or the use of specific tools "intrudes" on the agency's discretion. The idea that certain areas of a Federal department or agency would be "out of bounds" for a Federal Office of Inspector General to review and recommend corrective action runs counter to the spirit and letter of the IG Act and it's various amendments.

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

OPM's System Development Life Cycle (SDLC) policy was last updated in 2013 and to date is still not actively enforced for all IT projects. As noted in the FY 2017 OIG FISMA audit report, OPM's long history of troubled system development projects further emphasizes the need for OPM to develop a plan to enforce its SDLC policy. The OCIO's response to the FY 2017 audit recommendation discussed updating the SDLC policy prior to agency-wide distribution and enforcement. However, we were informed this year that the policy update has been put on hold due to organizational changes in the OCIO. The establishment of OPM's Enterprise Project Management Office (discussed in Metric 8) should allow the agency to provide better consistency across its system development projects once finalized SDLC policies and procedures are enacted.

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."

Despite a long history of troubled system development projects, OPM still does not consistently enforce a comprehensive SDLC.

The lack of an effective SDLC methodology increases the risk that OPM will waste resources on system development projects that will not meet the needs and/or requirements of the agency. It also increases the likelihood that adequate IT security controls are not built into a new system during the development process, resulting in a potentially insecure system.

Recommendation 18 (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. OPM recognizes the need to enforce its SDLC policy on all IT projects. As referenced by the OIG for this metric, OPM is establishing a new EPMO that will address this recommendation."

E. <u>CONFIGURATION MANAGEMENT</u>

Configuration Management (CM) controls allow an organization to establish information system configuration baselines, processes for securely managing changes to configurable settings, and procedures for monitoring system software. OPM did not improve its CM program in FY 2018. Furthermore, we have identified additional areas for improvement in this domain. The sections below detail the results for each individual metric in this domain. **<u>OPM's overall maturity level for the Configuration Management domain is "2 – Defined."</u>**

Metric 14 – Configuration Management Roles, Responsibilities, and Resources

<u>FY 2018 Maturity Level: 2 – Defined.</u> 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 resources (people, processes, and technology) to effectively manage its CM program. The resource constraints discussed in Section B and the inventory management and architecture issues discussed in Section C are two impediments to a successful CM program.

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.

<u>Recommendation 19 (Rolled forward from FY 2017)</u>

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.

<u>OPM Response:</u>

"We concur with the recommendation. As referenced by the OIG, OPM has already dedicated resources to establishing a new EPMO. Defining the resource requirements to effectively implement the configuration management program is one of the objectives of the effort."

Metric 15 – Configuration Management Plan

FY 2018 Maturity Level: 2 – Defined. OPM has developed a CM plan that outlines CM-related roles and responsibilities, establishes a change control board, and defines processes for implementing configuration changes. Additionally, OPM has established a process to document any lessons learned as a result of configuration changes, the overall change control process, and flaw remediation. However, while the agency does document lessons learned from its configuration change control process, it does not currently use these lessons to update and improve its configuration management plan as necessary.

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."

Recommendation 20 (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. OPM is in the process of establishing a new EPMO that will significantly modify its configuration management practices and create new planning tools. Given the transformation already underway in this area that will incorporate best practices based on lessons learned and other factors, OPM does not agree that this recommendation is timely or appropriate."

OIG Comment:

We support OPM's effort in developing new configuration management practices and creating new planning tools in an attempt to address this recommendation from last year. Once completed, please provide the appropriate and adequate evidence to OPM's Internal Oversight and Compliance office to support closure of this recommendation.

Metric 16 – Implementation of Policies and Procedures

FY 2018 Maturity Level: 2 – Defined. OPM has defined organization-wide CM policies and procedures, but has not consistently implemented many of the controls outlined in these policies, such as:

- Establishing and maintaining baseline configurations and inventories of information systems;
- Routinely verifying that information systems are actually configured in accordance with baseline configurations; and
- Conducting routine vulnerability scans on all information systems and remediating any vulnerabilities identified from the scan results in a timely manner.

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

Metric 17 – Baseline Configurations

FY 2018 Maturity Level: 1 – Ad-hoc. OPM has not developed a baseline configuration for all of its information systems. NIST SP 800-53, Revision 4, states that "Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture."

OPM 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, requires that an organization "develops, documents, [and] maintains under configuration control, a current baseline configuration of the information system."

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

Recommendation 21 (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. OPM is establishing a new EPMO that will address this recommendation."

Recommendation 22 (Rolled forward from 2017)

We recommend that the OCIO conduct routine compliance scans against established baseline configurations for all OPM information systems. This recommendation cannot be addressed until Recommendation 21 has been implemented.

OPM Response:

"We concur with this recommendation. OPM is establishing a new EPMO that will address this recommendation."

Metric 18 – Security Configuration Settings

FY 2018 Maturity Level: 1 – Ad-Hoc. DHS makes the distinction between implementing baseline configurations and implementing standard security configuration settings (see Metrics 17 - 18).

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 that "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."

While OPM has workstation and server build images that leverage common best-practice configuration setting standards, it has yet to document and approve standard security configuration settings for all of its operating platforms nor any potential business-required deviations from these configuration standards.

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.

Furthermore, without formally documented and approved configuration settings, OPM cannot consistently run automated scans to verify that information systems maintain compliance with the pre-established configuration settings. Security configuration setting scans can be configured to automatically check the current status of the various system parameters outlined above in the NIST definition of configuration settings. Automated 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 23 (Rolled forward from FY 2014)

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

OPM Response:

"We concur with the recommendation. OPM plans to expand and implement standard security configurations for all servers and databases."

Recommendation 24 (Rolled forward from FY 2014)

We recommend that the OCIO conduct routine compliance scans against [the standard security configuration settings] for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 23 has been completed.

OPM Response:

"We do not concur with the recommendation. The OCIO is currently conducting scans of OPM servers and databases. OCIO will continue the practice for any new security standards that we introduce or implement. The practice that OPM currently has in place is working appropriately and is consistent with security standards."

OIG Comment:

As noted in Metric 18, OPM does not have documented standard security configuration settings for its operating platforms and databases deployed in its technical environment. Without approved security configuration standards, OPM cannot effectively scan its system's security settings for deviations or unauthorized changes (i.e., there are no approved settings to which to compare the actual settings). Recommendations 23 and 24 have been open since FY 2014 because adequate and appropriate evidence has not been provided to OPM's Internal Oversight and Compliance office to support their closure. If the OCIO has addressed these recommendations, it should provide supporting documentation.

Recommendation 25 (Rolled forward from FY 2016)

For OPM configuration standards that are based on a pre-existing generic standard, we recommend that OPM document all instances where the OPM-specific standard deviates from the recommended configuration setting.

OPM Response:

"We concur with the recommendation. Increased ISSO resources will allow for expanded documentation and approval of deviations."

Metric 19 – Flaw Remediation and Patch Management

FY 2018 Maturity Level: 2 – Defined. OPM routinely performs automated vulnerability and patch compliance scans on its systems. While OPM's vulnerability scanning program has improved over the last year, our audit test work indicated that several problems still exist.

Specifically, OPM's scanning tool was unable to successfully scan certain devices within OPM's internal network. In addition, the results of our independent vulnerability scans indicate that OPM's production environment contains many instances of unsupported software and operating platforms. In other words, the software vendor no longer provides patches, security fixes, or updates for the software. As a result, there is an increased risk that OPM's technical environment contains known vulnerabilities that will never be patched, and could be exploited to allow unauthorized access to sensitive data.

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

OPM does not have a process to record or track the remediation status for weaknesses identified during vulnerability scans.

NIST SP 800-53, Revision 4, states that the 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 . . . ."

Additionally, during our vulnerability and compliance testing, we found multiple scenarios where administrator credentials in OPM's password repository failed to authenticate. This issue indicates that the agency does not have an adequate process to manage credentials for its administrator accounts used for scanning. Also, we determined that not every device on OPM's network is scanned routinely, nor is there a formal process in place to ensure that all new devices on the agency's network are included in the scanning process.

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

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

<u>Recommendation 26</u>

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

OPM Response:

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

Recommendation 27

We recommend that the OCIO implement a process for updating and maintaining credentials for its scanning accounts.

OPM Response:

"We do not concur with this recommendation because OCIO has already implemented a process for updating and maintaining credentials for its scanning accounts and provided information to reflect that implementation to the OIG in May 2018. Implementation occurred immediately following the conclusion of the prior year FISMA audit in response to the issuance of Recommendation 23 from the OIG Report 4A-CI-00-17-020."

OIG Comment:

During the course of our audit, we found significant weaknesses in the OCIO's management of scanning credentials. As noted in Metric 19, there were multiple instances during our scanning exercise in July 2018 where credentials failed to properly authenticate. After the scanning exercise, we requested additional information surrounding the management of scanning credentials. OPM's response indicated that changes to vendor contracts and its infrastructure would improve the process. While this may be true in the future, our audit clearly demonstrated that the current process for managing credentials is not effective. The recommendation cited in OPM's response is focused on OPM scanning all network devices and its closure would not necessarily address the issues that we have identified.

Recommendation 28 (Rolled forward from FY 2014)

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

OPM Response:

"We do not concur with this recommendation. As described under our response to Recommendation 27, OPM implemented a process for updating and maintaining credentials for its scanning accounts and provided information to reflect that implementation to the OIG in May 2018. Implementation occurred immediately following the conclusion of the prior year FISMA audit in response to the issuance of Recommendation 23 from the OIG Report 4A-CI-00-17-020."

OIG Comment:

Ensuring all devices on OPM's network are routinely scanned has been an ongoing issue. Again this year, our scanning exercise identified a number of network devices that are not subject to routine credentialed vulnerability scanning. Recommendation 28 is not the same as Recommendation 27 and the process needed to address this one would be very different from one that is used to address the credential management issue. During this audit, our review of the vulnerability scanning process did not reveal any significant changes that would address this recommendation. Additionally, OPM's Internal Oversight and Compliance office has not received evidence for consideration related to OIG Report No. 4A-CI-00-17-020, OPM's Compliance with Federal Information Security Modernization Act (FISMA) FY 2017, issued October 27, 2017.

Recommendation 29 (Rolled forward from FY 2016)

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

OPM Response:

"We partially concur with the recommendation. OPM understands we have unsupported software and operating systems; however, risk assessments and mitigating controls have been implemented by the agency so that detected vulnerabilities cannot be exploited. Additionally, projects are underway to remove unsupported software and systems from the network."

OIG Comment:

We do not agree that OPM's risk assessments and mitigating controls are enough to compensate for the risk of malicious exploitation of unsupported software and operating systems currently in OPM's production environment. We continue to find issues with OPM's system level risk assessments as discussed in Metric 9. Furthermore, OPM does not clarify the compensating controls that are in place to reduce the risk of unsupported software.

As mentioned in Metric 19, the software vendor no longer provides patches, security fixes, or updates for the software. As a result, there is an increased risk that OPM's technical environment contains known vulnerabilities that will never be patched, and could be exploited to allow unauthorized access to sensitive data.

Recommendation 30 (Rolled forward from FY 2014)

We recommend that the OCIO implement a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.

OPM Response:

"We do not concur with the recommendation because OPM has already implemented this type of process. The OIG states in the report that OPM does not have a process to record or track the remediation status for other routine security weaknesses identified during vulnerability scans. However, in February 2018, OPM developed a process for tracking the remediation status of weaknesses identified during vulnerability scans in response to the prior year audit. OPM intends to use this process until the DHS CDM program delivers automated data feeds to OPM's tracking repository."

OIG Comment:

OPM's Internal Oversight and Compliance office has not received evidence for consideration related to Recommendation 30 in the prior year's FISMA audit. OPM's response to our follow-up from the prior year's audit indicated that the implementation of this recommendation would not be completed until June 30, 2018. We have not seen evidence that implementation of this recommendation has been completed.

Recommendation 31 (Rolled forward from FY 2014)

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

OPM Response:

"We partially concur with the recommendation. The agency has a process for patch management to help ensure timely deployment of patches and has seen significant improvements in timeliness and an ability to routinize patch deployments over the past year. OCIO expects further improvements in timeliness over the upcoming year and will utilize enterprise change management processes. This change management process will include submissions of evidence supporting adherence to the processes. In the short term, a patch management tiger team plan is in draft form."

OIG Comment:

We fully support the OCIO's efforts in improving its patch management process. Please provide evidence to OPM's Internal Oversight and Compliance office when this patch management process is fully implemented.

Metric 20 – Trusted Internet Connection Program

FY 2018 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented controls to monitor and manage its approved trusted internet connections. This has allowed OPM to meet OMB requirements related to the trusted internet connections initiative. Any improvements that need to be made to the agency's current trusted internet connections controls are documented within the organization's POA&M.

OPM has implemented controls to monitor and manage its trusted internet connections.

Metric 21 – Configuration Change Control Management

FY 2018 Maturity Level: 3 – Consistently Implemented. OPM has developed and documented policies and procedures for controlling configuration changes. The policies address the necessary change control steps and required documentation needed to approve information system changes. Our test work indicated that OPM has updated its configuration change control process to include project plans and additional reviews and approvals and is consistently adhering to its change control procedures.

Metric 22 – Configuration Management Other Information

There are no additional comments regarding configuration management.

F. IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT

OPM has consistently implemented many ICAM related security controls.

The Federal Identity, Credential, and Access Management (FICAM) program is a government-wide effort to help Federal agencies provision access to systems and facilities for the right person, at the right time, for the right reason. While OPM still has work ahead in this area, it 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 2018 Maturity Level: 2 – Defined. OPM maintains policies and procedures that outline its agency-wide system account and identity management program roles and responsibilities. This includes procedures for creating user accounts with the appropriate level of access and procedures for removing access for terminated employees. However, as discussed in the Information Security Governance section of this report (see Section B), the OCIO has lost multiple key personnel in FY 2018 and has many vacant ISSO positions. As such, OPM does not have adequate resources (people, processes, and technology) in place to fully implement ICAM controls.

FICAM Roadmap Implementation Guidance states that "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 that "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 chances the agency will experience lapses in optimizing its ICAM strategy.

<u>Recommendation 32 (Rolled forward from FY 2017)</u>

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.

<u>OPM Response:</u>

"We partially concur with this recommendation. The agency does not consider ICAM to be a distinct program, though it could potentially be deemed a service area under the Security Operations Center Monitoring and Analysis team. The agency has initial plans on how to address this recommendation that can be incorporated as part of a long term strategy.

Further, the OIG references the loss of ISSOs as a reason for the lack of implementation of ICAM controls but does not explain the connection it has made between ISSO resourcing and the perceived limitations in the ICAM program. It is difficult for OPM to assess its response to this recommendation without further information."

<u>OIG Comment:</u>

Whether ICAM is treated as a distinct program or a service area under the Security Operations Center Monitoring and Analysis team, the intent and principles of ICAM need to be adequately addressed. OPM should evaluate if it has adequate resources necessary to design and implement its ICAM activities as intended.

Section B references loss of key personnel, including ISSOs. According to OPM's Access Control policy, ISSOs perform an important role related to account management and access monitoring; therefore, lack of resources would impact OPM's ability to follow through in the execution of ICAM activities.

Metric 24 – ICAM Strategy

<u>FY 2018 Maturity Level: 1 – Ad Hoc.</u> OPM has not developed an ICAM strategy that includes a review of current practices ("as-is" assessment), identification of gaps (from a desired or "to-be" state), and a transition plan.

According to FICAM Roadmap 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 lack of an ICAM strategy that includes a review of current practices, identification of gaps, and a transition plan can prevent OPM from ensuring the success of its ICAM initiatives. Although OPM has successfully implemented many ICAM-related controls, the development of a comprehensive ICAM strategy will ensure the ongoing success of the agency's ICAM program.

Recommendation 33 (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 partially concur with this recommendation. The agency does not consider ICAM to be a distinct program though it could potentially be deemed a service area under the Security Operations Center Monitoring and Analysis team. The agency has initial plans on how to address this recommendation that can be incorporated as part of a long term strategy."

OIG Comment:

We support OPM's efforts in developing a long term ICAM strategy. Whether ICAM is treated as a distinct program or a service area under the Security Operations Center Monitoring and Analysis team, the intent and principles of ICAM need to be adequately addressed and executed.

Metric 25 – Implementation of an ICAM Program

FY 2018 Maturity Level: 3 – Consistently Implemented. OPM has consistently implemented many of the required elements of a comprehensive ICAM program (see Metrics 26 - 31). However, OPM has not implemented Personal Identity Verification (PIV) authentication at the application level (see Metric 28), and does not adequately manage contractor accounts (see Metric 32). Furthermore, OPM policies do not address the capturing and sharing of lessons learned on the effectiveness of the agency's ICAM program.

According to the FICAM Roadmap Implementation Guidance, “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.”

An inability to consistently capture and share lessons learned on the effectiveness of an ICAM program will decrease the speed and efficiency in which it is implemented.

Recommendation 34 (Rolled forward from FY 2017)

We recommend that OPM implement a process to capture and share lessons learned on the effectiveness of its ICAM policies, procedures, and processes to update the program.

OPM Response:

“We partially concur with this recommendation. The agency does not consider ICAM to be a distinct program though it could potentially be deemed a service area under the Security Operations Center Monitoring and Analysis team. The agency has initial plans on how to address this recommendation that can be incorporated as part of a long term strategy.”

OIG Comment:

We support OPM’s efforts in developing a long-term ICAM strategy. Whether ICAM is treated as a distinct program or a service area under the Security Operations Center Monitoring and Analysis team, the intent and principles of ICAM need to be adequately addressed and executed.

Metric 26 – Personnel Risk

FY 2018 Maturity Level: 4 – Managed and Measurable. OPM has defined and implemented processes for assigning personnel risk designations and performing appropriate screenings prior to granting access to its systems. OPM has also implemented an automated process to centrally document, track, and share risk designations and screening information with necessary parties. OPM has procedures to re-screen individuals when they change positions or the risk designation of their current position is changed.

Metric 27 – Access Agreements

__FY 2018 Maturity Level: 3 – Consistently Implemented__. OPM has defined and implemented its processes for developing, documenting and maintaining access agreements for all users of the network. These access agreements are completed prior to granting any network or system access. The agency also utilizes detailed agreements for privileged users or those with access to sensitive information, as appropriate.

Metric 28 – Multi-factor Authentication with PIV

__FY 2018 Maturity Level: 3 – Consistently Implemented.__ OMB Memorandum M-11-11 required all Federal information systems to use Personal Identity Verification (PIV) credentials for multi-factor authentication by the beginning of FY 2012. In addition, the memorandum stated that all new systems under development must be PIV compliant prior to being made operational.

OPM has enforced multi-factor authentication for non-privileged users for facility, network, and remote access through the use of PIV cards. The FY 2018 FISMA metrics state that these controls represent a "consistently implemented" strong authentication mechanism. In order to reach the next level of maturity, the enforcement of PIV authentication to connect to the agency's network in itself is not a sufficient control, as users or attackers that do gain access to the network can still access OPM applications containing sensitive data with a simple username and password. If the back-end applications were configured to only allow PIV authenticated users, an attacker would have extreme difficulty gaining unauthorized access to data without having physical possession of an authorized user's PIV card.

OPM has not enforced PIV authentication to the vast majority of its applications.

Recommendation 35 (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.

OPM Response:

"We concur with the recommendation. The OCIO has plans to deploy an identity and access tool to assist with meeting OMB M-11-11."

Metric 29 – Strong Authentication Mechanisms for Privileged Users

FY 2018 Maturity Level: 3 – Consistently Implemented. OPM has enforced multi-factor authentication for privileged user access to the OPM network and its backend servers.

Metric 30 – Management of Privileged User Accounts

FY 2018 Maturity Level: 3 – Consistently Implemented. OPM has developed and implemented processes for provisioning, managing, and reviewing privileged user accounts. Account sessions are recorded, logged and reviewed periodically. OPM has placed restrictions on the functions that can be performed from privileged user accounts, and also restricts the session time.

Metric 31 – Remote Access Connections

FY 2018 Maturity Level: 4 – Managed and Measurable. OPM has implemented a variety of controls for remote access connections such as the use of cryptographic modules, system time outs, and monitoring remote access sessions. The agency ensures that remote access users' activities are logged and reviewed periodically. In addition, OPM ensures that user devices have been appropriately configured prior to allowing remote access, and restricts the ability of individuals to transfer data accessed remotely to non-authorized devices.

Metric 32 – ICAM Other Information – Contractor Access Management

OPM has defined and implemented processes for managing Federal employees' physical and logical access to sensitive resources. However, the process for terminating access for contractors leaving the agency is not centrally managed, and it is the responsibility of the various contracting officer representatives to notify the OCIO that a contractor no longer requires 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 that contractor accounts are removed in a timely manner.

The Federal Information System Controls Audit Manual 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 36 (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 policy requirements into tool deployment. Use of this tool will also aid in auditing of user accounts."

G. 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. This is a new domain area for the FY 2018 FISMA metrics and maturity models. 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 2018 Maturity Level: 1 – Ad Hoc. The OPM Information Security and Privacy Policy Handbook is OPM's primary source for data protection and privacy policies. However, this handbook has not been updated since 2011 and does not contain the personally identifiable information (PII) protection plans, policies, and procedures necessary for a mature privacy program. Additionally, there is an inadequate number of staff currently within OPM's privacy program. OPM's privacy program is supported by the Chief Privacy Officer, and two detailees from the OCIO. The Chief Privacy Officer position was established in October of 2016. Additional roles and responsibilities needed have not been clearly defined to support the program.

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

Without a strong privacy program in place, OPM increases the agency's risk for data loss and mishandling of sensitive information.

Recommendation 37

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

OPM Response:

"We partially concur. We agree that in order for the privacy program to develop into a more robust program, additional resources along with more clearly articulated roles and responsibilities are needed, both in the office that has immediate responsibility for privacy matters and throughout OPM. We disagree that no roles and responsibilities for privacy are currently defined at OPM. OPM elevated the Chief Privacy Officer/Senior Agency Official for Privacy to a senior-level position reporting directly to the Director of OPM. That position, based on the position description and the requirements set forth in guidance from the Office of Management and Budget, has responsibility for privacy policy and compliance at OPM."

OIG Comment:

OPM and the OIG are in agreement that roles and responsibilities need to be more clearly defined in order to implement a robust privacy program. As mentioned in Metric 33, we acknowledge that a Chief Privacy Officer is in place. However, additional roles and responsibilities have not been defined to support the program. In order for the Chief Privacy Officer to carry out the responsibilities of the agency's privacy program, roles and responsibilities should be defined. We support OPM's continued efforts to address data protection and privacy.

Recommendation 38

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. We agree that a more focused articulation of privacy policies and procedures that are separate from and/or integrated with information security policy and procedures, as appropriate, will be beneficial and we are working towards that end. We disagree that there are not currently in place plans, policies, and procedures for the protection of PII. The Information Security and Privacy Policy Handbook includes appropriate privacy provisions, as do the current PIA and SORN guides. In addition, the Chief Privacy Officer

implemented a robust template for Privacy Impact Assessments (PIA) that has been in use since calendar year 2017, as well as a new template for Privacy Threshold Analyses (PTA). The PTA template has been implemented both to determine the need for a PIA or a Privacy Act system of records notice and to track appropriate privacy controls as articulated in NIST 800-53, Appendix J. In addition to those OPM-specific policies and procedures, the agency continues to rely on overarching privacy guidance issued by the Office of Management and Budget and NIST."

OIG Comment:

We do not agree with OPM that the current policies, plans, and procedures in place are working to ensure the protection of PII. The material in the Information Security and Privacy Policy Handbook does not reflect the current state of OPM's privacy program since this policy has not been updated/reviewed since 2011. Furthermore, during our discussions with OCIO we learned that there are many system Authorizations in place without an approved Privacy Threshold Analysis.

Metric 34 – Data Protection and Privacy Controls

FY 2018 Maturity Level: 1 – Ad Hoc. DHS requires the implementation of several technical controls to help protect PII. OPM has implemented technical controls to limit the transfer of information via removable media, but has not provided sufficient evidence to demonstrate that controls to encrypt data at rest and in transit have been implemented in order to protect PII.

NIST SP 800-53, Revision 4, states that "The information system protects the [confidentiality and integrity] of [information at rest]." Furthermore, NIST SP 800-53, Revision 4, states that "The information system protects the [confidentiality and integrity] of transmitted information." Without strong security controls to protect PII, OPM increases its risk of cybersecurity threats and loss of information.

Recommendation 39

We recommend that OPM implement controls over encryption of data at rest on its IT systems.

OPM Response:

"We do not concur with this recommendation. OPM has implemented controls over encryption of data at rest on its IT systems. The OIG has not yet provided OPM with a clear understanding of what evidence is needed to demonstrate that controls over encryption of data at rest on its IT systems are in place."

OIG Comment:

No evidence was provided to the OIG during this audit demonstrating that OPM has controls in place to encrypt data at rest. The information request that we provided to OPM stated that screenshots demonstrating functionality, descriptions, and procedures would have been adequate evidence. Please provide OPM's Internal Oversight and Compliance office the appropriate and adequate evidence to close this recommendation.

Recommendation 40

We recommend that OPM implement controls over encryption of data in transit on its IT systems.

OPM Response:

"We do not concur with this recommendation. OPM has implemented controls over encryption of data in transit on its IT systems. The OIG has not yet provided OPM with a clear understanding of what evidence is needed to demonstrate that controls over encryption of data at rest on its IT systems are in place."

OIG Comment:

No evidence was provided to the OIG during this audit demonstrating that OPM has controls in place to encrypt data in transit. The information request that we provided to OPM stated that screenshots demonstrating functionality, descriptions, and procedures would have been adequate evidence. Please provide OPM's Internal Oversight and Compliance office the appropriate and adequate evidence to close this recommendation.

Metric 35 – Data Exfiltration Prevention

FY 2018 Maturity Level: 1 – Ad Hoc. OPM has implemented controls to monitor inbound and outbound network traffic, as well as ensure all traffic passes through a web content filter. However, OPM has not developed or defined its policies and procedures related to data exfiltration or enhanced network defenses.

DHS requires that the organization define and communicate its policies and procedures related to data exfiltration and network defenses.

Failure to develop and implement policies and procedures related to data exfiltration increases the risk of the organization mishandling data and the likelihood of data loss through user error.

Recommendation 41

We recommend that OPM develop and implement policies and procedures related to data exfiltration and enhanced network defenses.

OPM Response:

"We do not concur with this recommendation. OPM has issued several policies covering the data exfiltration and enhanced network defenses, including: 1) Information System Monitoring; 2), OPM Boundary Protection; 3) OPM Malicious Code; and 4) Mobile Code."

OIG Comment:

Current policies and procedures related to OPM's data protection and privacy program were requested during our audit. However, as of August 1, 2018, OPM did not provide the policies and procedures mentioned in their response. Therefore, we cannot express an opinion as to whether the policies and procedures are adequate. Please provide OPM's Internal Oversight and Compliance office the appropriate and adequate evidence to close this recommendation.

Metric 36 – Data Breach Response Plan

FY 2018 Maturity Level: 2 – Defined. OPM has defined and communicated its Data Breach Response Plan and established a data breach response team. However, OPM does not currently conduct routine table-top exercises to test the Data Breach Response Plan.

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

Failure to test the Data Breach Response Plan increases the organization's risk of major data loss in the event of a security incident.

Recommendation 42

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

OPM Response:

"We partially concur. We agree that an annual table top exercise to review the Breach Response Plan can help clarify and refine roles and responsibilities in the event of a breach and help to more clearly articulate the appropriate risk analysis and mitigation steps that should be taken, as provided by the Breach Response Plan and OMB Memorandum 17-12. We disagree with the OIG's underlying premise that not conducting a table top exercise has increased OPM' s risk of major data loss in the event of a security incident. Annual security and privacy awareness training informs the OPM workforce of when to report a loss or potential loss of PII to the Security Operations Center (SOC). The SOC routinely informs appropriate OPM personnel when an incident has occurred and steps are taken to address and mitigate any potential harm as appropriate. The Chief Privacy Officer is also a part of the senior members of the OPM staff that routinely meets and interacts with other key members of the workforce, which allows for consistent communication regarding the protection of sensitive identifiable information to occur."

OIG Comment:

Routine testing of the Data Breach Response Plan is a characteristic of a mature security posture and will help ensure that OPM's Data Breach Response Plan is working as intended. Furthermore, as in the past, OPM did not properly notify the OIG of several recent security incidents, suggesting that the Data Breach Response Plan is not always followed appropriately and should be routinely tested.

Metric 37 – Privacy Awareness Training

FY 2018 Maturity Level: 2 – Defined. OPM has defined and communicated its privacy awareness training program throughout the agency. OPM tailors the training to the organization's risk environment, ensures that all employees receive basic privacy awareness training on an annual basis, and requires all users to accept a rules of behavior notice prior to logging onto the network. However, individuals with responsibilities for PII or activities involving PII do not receive elevated role-based privacy training.

NIST SP 800-122 requires 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."

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

Not providing specific training to individuals who handle PII increases the organization's risk of mishandled secure data resulting in a data loss incident.

Recommendation 43

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. We agree that appropriate annual privacy training should be provided. This is done formally through the annual security and privacy awareness training that all individuals at OPM are required to complete. We also agree that it would be beneficial to evaluate more formally whether there are individuals who, given their job responsibilities and exposure to PII, should receive any additional annual training. We disagree with the underlying assumption that individuals who regularly handle PII will always require specialized formal annual training. In many instances the annual awareness training, followed by tailored discussions with various offices, can be just as effective. To date, the Chief Privacy Officer has provided presentations on privacy and engaged in group discussions with various offices in an effort to further provide appropriate privacy awareness and compliance."

OIG Comment:

This recommendation was made in alignment with DHS's requirement that role-based privacy training be conducted at least annually for individuals with responsibilities for PII. Furthermore, no evidence was provided during this audit demonstrating the ad-hoc training described in OPM's response. Please provide OPM's Internal Oversight and Compliance office the appropriate and adequate evidence to close this recommendation.

Metric 38 – Other Information Data Protection and Privacy

There are no additional comments regarding data protection and privacy.

H. SECURITY TRAINING

FISMA requires that all Government employees and contractors take annual IT security awareness training. In addition, employees with IT security responsibility are required to take specialized training specific to their job function. OPM has a strong history of providing its employees with IT security awareness training for the ever changing risk environment and has made progress in providing tailored training to those with significant security responsibilities. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Security Training domain is "3 – Consistently Implemented."**

Metric 39 – Security Training Policies and Procedures

FY 2018 Maturity Level: 3 – Consistently Implemented. OPM has developed and established an agency-wide IT security awareness training program. Roles and responsibilities for stakeholders are defined and communicated across the organization. OPM is continuing to improve its security training program by developing a process to consistently collect, monitor, and analyze qualitative and quantitative performance measures of the security awareness training activities.

We noted no control deficiencies during our review of the agency's security awareness training policies and procedures.

Metric 40 – Assessment of Workforce

FY 2018 Maturity Level: 1 – Ad Hoc. Since FY 2017, OPM has conducted an assessment of the knowledge, skills, and abilities of its workforce to determine employees' specialized training needs. While progress has been made, OPM still needs to analyze the results of the assessment to determine any skill gaps and specialized training needs.

The Federal Cybersecurity Workforce Assessment Act of 2015 requires agencies to implement "a strategy for mitigating any gaps identified . . . with appropriate training and certification for existing personnel."

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

Recommendation 44 (Rolled forward from 2017)

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

OPM Response:

"We concur with this recommendation. OPM completed the assessment of its workforce's knowledge, skills, and abilities in accordance with the instructions given for the Federal Cybersecurity Workforce Assessment Act of 2015. This assessment was completed in August 2018, after the OIG audit testing period, and can be provided upon request."

Metric 41 – Security Awareness Strategy

FY 2018 Maturity Level: 3 – Consistently Implemented. In FY 2018, OPM developed a strategic plan for the cybersecurity policy team, which includes security awareness training. The strategy has been fully developed to maintain a security awareness program tailored to the mission and risk environment.

Based upon our review of the agency's Security Awareness and Training Strategy and its implementation, no control deficiencies were noted.

Recommendation 45 (Rolled forward from 2017)

We recommend that OPM develop and document a security awareness and training strategy tailored to its mission and risk environment.

OPM Response:

We do not concur with this recommendation. The Security Awareness and Training Strategy was completed in May 2018 and was delivered to the OIG in June 2018. OPM's view is that the strategy is appropriately tailored to the agency mission and risk environment.

OIG Comment:

This recommendation was rolled forward from FY 2017 based on our meeting discussions that indicated the Security Awareness and Training Strategy was still a work in progress. However, after consideration of OPM's response to the draft audit report and review of the documentation provided to us during the audit we have determined that sufficient evidence has been provided to close the recommendation from 2017, and no further action is required.

Metric 42 – Specialized Security Training Policies

FY 2018 Maturity Level: 3 – Consistently Implemented. OPM has established policies and procedures that require agency employees to take security awareness and specialized security training. OPM is working to improve its security training program by implementing a process to measure the effectiveness of specialized training.

Based upon our review of the agency's specialized security awareness training policies and procedures, no control deficiencies were noted.

Metric 43 – Tracking IT Security Training

FY 2018 Maturity Level: 4 – Managed and Measureable. The OCIO provides annual IT security and privacy awareness training to all OPM users through an interactive web-based course. The course introduces employees and contractors to the basic concepts of IT security and privacy, including topics such as the importance of information security, security threats and vulnerabilities, viruses and malicious code, privacy training, telework, mobile devices, Wi-Fi guidance, and the roles and responsibilities of users. In addition, OPM conducts random phishing exercises and tracks the results in order to measure the effectiveness of the exercises. Lessons learned are reviewed and used to update the IT security training program. Over 95 percent of OPM's employees and contractors completed the security awareness training course in FY 2018.

Over 95 percent of OPM employees and contractors completed security awareness training.

Metric 44 – Tracking Specialized IT Security Training

FY 2018 Maturity Level: 3 – Consistently Implemented. 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 spreadsheet to track the security training taken by employees identified as having security responsibility. In order to improve the specialized training program, the OCIO is in the process of developing metrics to measure the effectiveness of the specialized training program.

Metric 45 – Security Training Other Information

There are no additional comments regarding the security training program.

I. INFORMATION SECURITY CONTINUOUS MONITORING

Information Security Continuous Monitoring (ISCM) controls involve the ongoing assessment of the effectiveness of information security controls in support of the agency's efforts to manage 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 2018 Maturity Level: 2 – Defined. OPM has developed an ISCM strategy that addresses the monitoring of security controls at the organization, business unit, and individual information system level. At the organization and business unit level, the ISCM strategy defines how the agency's activities support risk management in accordance with organizational risk tolerance. At the information system level, the ISCM strategy establishes processes for monitoring security controls for effectiveness and reporting any findings.

Despite a defined ISCM strategy, OPM is not consistently implementing several of the objectives outlined in its ISCM strategy, including:

- "Security controls must be assessed to ensure continued effectiveness of their implementation and operation";

- "Identified threats and vulnerabilities must be reported timely to support risk management decisions"; and

- "Feedback must be collected frequently and incorporated into a system of continually improving processes."

In FY 2018 only 29 of OPM’s 54 systems were subject to adequate security controls testing and monitoring.

At this stage in the development of OPM’s ISCM program the goal of providing stakeholders with sufficient information to evaluate risk has not been met. Ensuring that the security controls of each system are assessed on a continuous basis is the responsibility of the ISSO for each major system. ISSOs should be both competent and knowledgeable, and the overall program should be properly managed. As discussed in Section B, we continue to believe that OPM’s failure to meet long-standing FISMA metrics (such as the ones in this section related to continuous monitoring) is a direct result of OPM’s inability to fully staff critical information security positions, and is indicative of a material weakness in the agency’s governance structure.

Only 29 of OPM’s 54 systems were subject to adequate security controls testing and monitoring.

Metric 47 – ISCM Policies and Procedures

FY 2018 Maturity Level: 2 – Defined. OPM has developed ISCM policies and procedures that have been tailored to OPM’s environment and include specific requirements and deliverables. However, OPM does not capture lessons learned to make improvements to ISCM policies and procedures. In addition, as discussed in more detail under Metric 49, OPM has not consistently implemented its ISCM policies.

Metric 48 – ISCM Roles, Responsibilities, and Resources

FY 2018 Maturity Level: 2 – Defined. OPM has defined the structure, roles, and responsibilities of its ISCM teams and stakeholders. However, we found that OPM’s ISCM program still does not have adequate resources to effectively implement the activities required. This year, OPM made some progress identifying resource gaps related to its ISCM program. However, more work is still required to identify all of the ISCM resource gaps to effectively implement its ISCM program.

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

Failure to identify and apply the resources needed to perform ISCM activities results in OPM being unable to effectively implement its ISCM program, limiting its ability to protect sensitive information.

Recommendation 46 (Rolled forward from 2017)

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

OPM Response:

"We partially concur with this recommendation. OPM agrees that challenges in resources have affected the ISCM program. OPM has identified needs and have responded by recruiting and making plans to bring onboard additional personnel."

OIG Comment:

As noted in Metric 48, OPM has made some progress identifying resource gaps related to its ISCM program. However, no evidence has been provided to us indicating that this recommendation has been fully implemented. Please provide OPM's Internal Oversight and Compliance office the appropriate and adequate evidence to close this recommendation.

Metric 49 – Ongoing Security Assessments

FY 2018 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, we continue to find that many system owners are not following the security control testing schedule that the OCIO mandated for all systems. OPM's policy requires that evidence of security control testing be provided to the OCIO on a quarterly basis for all OPM-operated systems, and annually for all contractor-operated systems.

We submitted requests for the security control testing documentation for all OPM systems in order to review them for quality and consistency. However, we were only provided evidence for the first two quarters of FY 2018. In those two quarters, only 29 of OPM's 54 major systems were subject to security controls testing that complied with OPM's ISCM submission schedule. While this would represent an improvement in the first half of the fiscal year compared to FY 2017, we were not provided any evidence for the third quarter.

While resource limitations certainly impact OPM's cybersecurity program, we believe that lack of effective management is a contributing factor. Monitoring status, following up on incomplete results, evaluating the quality of work products, and reporting to senior leadership and other stakeholders are basic elements of a properly managed program. OPM has not been able to adequately test the security controls of its systems for at least 10 years. In addition, OPM has not been able to implement continuous monitoring of its major IT systems since 2011 when it was required by NIST SP 800-37, Revision 1.

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

By failing to complete a comprehensive security controls test for all information systems and use the results to establish a risk baseline for the agency, 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 had security controls testing been completed.

Recommendation 47 (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 this recommendation. OPM agrees that challenges in resources have affected annual control testing. Additional resources joining the OCIO in the near future will help to ensure thorough annual security control testing for all systems."

Metric 50 – Measuring ISCM Program Effectiveness

FY 2018 Maturity Level: 2 – Defined. OPM has identified and defined the performance measures and requirements to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. OPM has also developed metrics to assess the program implementation and intends to consolidate reported data into a single repository as an efficient means to track the progress.

OPM must consistently test its systems' security controls before it can implement a mature continuous monitoring program.

However, OPM still needs to define the format and frequency of reports measuring its ISCM program effectiveness. In addition, OPM has failed to complete the first step necessary to assess the effectiveness of its ISCM program – to collect the necessary baseline data by actually assessing the security controls of its systems. To reach the next level in the ISCM maturity model OPM has to consistently capture the performance measures needed to evaluate the effectiveness of the ISCM program.

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

Recommendation 48 (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 47.

OPM Response:

“We do not concur with this recommendation. Performance measures for the ISCM program have been established and the OCIO is conducting an evaluation of the management of POA&Ms and inventory management. The use of a centralized tool is expected to provide a significantly expanded capability for evaluation.”

OIG Comment:

No evidence was provided during the course of this audit to indicate that qualitative and quantitative performance measures on the performance of its ISCM program have been implemented. Please provide OPM’s Internal Oversight and Compliance office the appropriate and adequate evidence to close this recommendation.

Metric 51 – ISCM Other Information

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

J. INCIDENT RESPONSE

OPM has an effective incident response program.

An incident response capability is an organized approach for responding 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 2018 Maturity Level: 4 – Managed and Measureable. OPM's incident response policies, procedures, plans, and strategies have been defined, communicated, and consistently implemented. OPM is consistently capturing and sharing lessons learned on the effectiveness of its incident response program. In addition, OPM monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response program and, as appropriate, implements updates to the program.

Metric 53 – Incident Roles and Responsibilities

FY 2018 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 2018 Maturity Level: 3 – Consistently Implemented. OPM utilizes a threat vector classification system for its incident response program, allowing the agency to quickly analyze and prioritize any incidents reported or detected. In addition, OPM has implemented several security tools to analyze precursors and indicators of security threats to help it better identify possible security incidents before they occur. However, OPM has not implemented profiling techniques to measure the characteristics of expected activities on its networks and systems so that it can effectively detect security incidents.

Metric 55 – Incident Handling

FY 2018 Maturity Level: 4 – Managed and Measureable. OPM has defined its processes for incident handling in an incident response manual. The processes include containment strategies for various types of major incidents, eradication activities to eliminate components of an incident and mitigate any vulnerabilities that were exploited, and the recovery of systems. OPM uses metrics to measure the impact of successful incidents and is able to quickly mitigate related vulnerabilities on other systems so that they are not subject to the same exploitation.

Metric 56 – Sharing Incident Response Information

FY 2018 Maturity Level: 4 – Managed and Measureable. OPM has a documented policy that defines how incident response information will be shared with individuals with significant security responsibility. OPM also has controls in place to generally ensure that security incidents are reported to the United States Computer Emergency Readiness Team, law enforcement, the OIG, and the Congress in a timely manner. OPM has developed and implemented incident response metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders. However, we have noticed incidents where OPM has failed to properly notify the OIG of security incidents in accordance with the defined process.

Metric 57 – Contractual Relationships in Support of Incident Response

FY 2018 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 2018 Maturity Level: 4 – Managed and Measureable. OPM has implemented incident response tools that have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures. OPM utilizes the reporting tools for monitoring and analyzing qualitative and quantitative incident response performance across the organization. OPM uses the data collected from these tools to generate monthly reports to stakeholders on the effectiveness of its incident response program.

Metric 59 – Incident Response Other Information

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

K. 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 2018 Maturity Level: 2 – Defined. OPM has a policy in place that describes the roles and responsibilities of individuals that are part of the agency's contingency planning program. OPM also uses a contingency plan template to develop consistent system level contingency plans. These policies, procedures, and templates are readily available to OPM personnel. However, the personnel limitations discussed in Section B are further evident in OPM's inability to perform all contingency planning activities.

NIST SP 800-34, Revision 1, states, "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 49

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

OPM Response:

"We do not concur with the recommendation. The OCIO is aware of the technology and resource gaps related to enterprise disaster recovery testing that can result in an ability to further plan development and conduct exercises and is taking steps, supported by agency leadership, to eliminate those gaps. The OIG cites ISSO staffing issues as reason for contingency plan development and testing weaknesses but does not explain how it has reached this conclusion."

OIG Comment:

The OCIO has repeatedly cited the lack of personnel resources as a substantial cause of its inability to address this recommendation. In addition to the loss of many ISSO positions, Section B of this report discusses the loss of multiple key individuals. For example, OPM's Data Center Group Chief, who played a pivotal role with contingency planning efforts, has recently left the agency. ISSOs perform an important role and impact OPM's ability to follow through in the execution of contingency activities. Conducting a gap analysis would be a prudent step to document the need and support requests for additional staff.

Metric 61 – Contingency Planning Policies and Procedures

FY 2018 Maturity Level: 2 – Defined. OPM has contingency planning policies and procedures in place, but does not consistently adhere to these policies. The remaining metrics in this domain outline the specific deficiencies in OPM's contingency planning program, but in summary:

- Contingency plans exist for only 32 of OPM's 54 major information systems;
- Only 19 of the 32 contingency plans were reviewed and updated in FY 2018;
- Only 13 of the 32 contingency plans were tested in FY 2018; and
- Only 1 contingency plan was updated to address the test results.

OPM's failure to test the contingency plans for almost 80 percent of its systems is a symptom of the significant deficiency in the agency's information security governance structure.

It is the responsibility of the ISSO for each major system to ensure that the system is subject to a contingency plan test each year and that the plan is updated accordingly. As discussed in Section B, we continue to believe that OPM's failure to meet long-standing FISMA metrics (such as the ones in this section related to contingency planning) is indicative of a material weakness in the agency's information security governance structure.

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

Metric 62 – Business Impact Analysis

FY 2018 Maturity Level: 1 – Ad-Hoc. Identifying an organization's essential mission and the risks facing its business functions is a critical element in developing contingency plans. OPM currently has a process in place to develop a Business Impact Analysis (BIA) at the information system level. While OPM has a substantial number of information systems that do not have an approved BIA, those systems have existing POA&Ms identifying these weaknesses.

Additionally, OPM has not performed an agency-wide BIA, and therefore, risks to the agency as a whole are not incorporated into the system-level BIAs and/or contingency plans. Currently, OPM is in the preliminary planning stages for its enterprise-wide contingency planning efforts that will include a BIA.

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

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

Without an organization-wide BIA, the agency leaves itself at risk of being unable to restore systems based on criticality, and therefore, unable to meet its recovery time objectives and mission.

Recommendation 50 (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.

OPM Response:

"We do not concur with the recommendation. OPM completed an agency-wide BIA and developed a new template with instructions for incorporating the results into system-level contingency plans in May 2018. The document can be provided upon request."

OIG Comment:

During the course of audit fieldwork, the OIG was not provided evidence that OPM completed an agency-wide BIA. As part of the audit resolution process, please provide OPM's Internal Oversight and Compliance office with evidence that this recommendation has been implemented.

Metric 63 – Contingency Plan Maintenance

FY 2018 Maturity Level: 2 – Defined. OPM has a policy that requires a contingency plan to be in place for every major information system, and that this plan be updated on a routine basis. While OPM has made progress, OPM is still far from adhering to this policy. In FY 2018, we received evidence that a contingency plan exists for 32 of OPM's 54 major systems. However, of those 33 contingency plans, only 19 were current, having been reviewed and updated in FY 2018.

The OPM contingency planning policy requires that Contingency planning procedures shall be developed and disseminated [and] the procedures shall be reviewed at least annually.

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

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

Recommendation 51 (Rolled forward from 2014)

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

OPM Response:

"We concur with the recommendation. The OCIO will coordinate with each system's Program Management Office (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."

Metric 64 – Contingency Plan Testing

FY 2018 Maturity Level: 2 – Defined. Routinely testing contingency plans is a critical step in ensuring that plans can be successfully executed in the event of a disaster. Only 13 of the 54 major information systems were subject to an adequate contingency plan test in fiscal year 2018. Furthermore, contingency plans for 17 of the 54 major systems have not been tested for 2 years or longer.

The OPM Contingency Planning Policy states that system owners must "test the contingency plan for the information system [at least annually] . . . ."

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

Recommendation 52 (Rolled forward from 2008)

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

OPM Response:

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

Metric 65 – Information System Backup and Storage

FY 2018 Maturity Level: 3 – Consistently Implemented. OPM has implemented processes, strategies, and technologies for information system backup and storage. OPM's systems are backed up to alternative storage sites that are documented within each system's security plan.

Metric 66 – Communication of Recovery Activities

FY 2018 Maturity Level: 2 – Defined. OPM has policies in place that define how contingency plan activities are performed throughout the agency. As discussed in Metric 61, these policies and procedures are distributed to all relevant stakeholders. However, OPM is not consistently adhering to this policy, as current contingency plans are not maintained for all systems.

The OPM contingency planning policy states that "Contingency planning procedures shall be developed and disseminated. The procedures shall be reviewed at least annually . . . ."

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

Failure to disseminate a complete and current contingency plan to key stakeholders increases the risk that the agency is unable to efficiently restore operations in the event of a disaster.

Recommendation 51 addresses the deficiencies in this metric.

Metric 67 – Contingency Planning Other Information

There are no additional comments regarding contingency planning.

APPENDIX I – Detailed FISMA Results by Metric

Metric Number and Description	Metric Maturity Level	Domain Maturity Level	Function Maturity Level	U.S. OPM Overall Maturity Level
1 - Inventory of Major Systems and System Interconnections	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	2			
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	2			
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	3			
26 - Personnel Risk	4			
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	1			
35 - Data Exfiltration Protection	1			
36 - Data Breach Response Plan	2			
37 - Privacy Awareness Training	2			
38 - Other Information - Data Protection and Privacy	n/a			
39 - Security Training Policies and Procedures	3	Security Training Level 3: Consistently Implemented		
40 - Assessment of Workforce	1			
41 - Security Awareness Strategy	3			
42 - Specialized Security Training Policies	3			
43 - Tracking IT Security Training	4			
44 - Tracking Specialized IT Security Training	3			
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	1			
63 - Contingency Plan Maintenance	2			
64 - Contingency Plan Testing	2			
65 - Information System Backup and Storage	3			
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 2017 FISMA audit (Report No. 4A-CI-00-17-020, issued October 27, 2017).

Rec #	Original Recommendation	Recommendation History	Current Status
1	We recommend that OPM hire a sufficient number of ISSOs to adequately support all of the agency's major information systems.	New recommendation for FY 2016	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 1
2	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-00-18-038 Recommendation 3
3	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-00-18-038 Recommendation 4
4	We recommend that the OCIO ensure that all ISAs are valid and properly maintained.	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 6
5	We recommend that the OCIO ensure that a valid MOU/A exists for every interconnection.	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 7
6	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 in FY 2016	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 8
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.	New recommendation for FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 10

8	We recommend that OPM define and communicate a risk management strategy based on the requirements outlined in NIST SP 800-39.	New recommendation for FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 11
9	We recommend that OPM update its enterprise architecture to include the information security architecture elements required by NIST and OMB guidance.	New recommendation for FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 12
10	We recommend that OPM continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive (Function).	Rolled forward from FY 2011	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 13
11	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-00-18-038 Recommendation 14
12	We recommend that OPM update its POA&M entries to reflect both the original and updated remediation deadlines 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).	New recommendation for FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 15
13	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 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 16
14	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.	New recommendation in FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 17
15	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-00-18-038 Recommendation 18
16	We recommend that OPM perform a gap analysis to determine the configuration management	New recommendation in FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 19

	resource requirements (people, processes, and technology) necessary to effectively implement the agency’s CM program.		
17	We recommend that OPM document the lessons learned from its configuration management activities and update its configuration management plan as appropriate.	New recommendation in FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 20
18	We recommend that OPM develop and implement baseline configuration for all information systems in use by OPM.	New recommendation in FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 21
19	We recommend that the OCIO conduct routine compliance scans against established baseline configurations for all OPM information systems. This recommendation cannot be addressed until Recommendation 18 has been implemented.	New recommendation in FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 22
20	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-00-18-038 Recommendation 23
21	We recommend that the OCIO conduct routine compliance scans against [the standard security configuration settings] for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 20 has been completed.	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 24
22	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-00-18-038 Recommendation 25
23	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-00-18-038 Recommendation 28
24	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-00-18-038 Recommendation 29

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-00-18-038 Recommendation 30
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-00-18-038 Recommendation 31
27	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.	New recommendation in FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 32
28	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.	New recommendation in FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 33
29	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.	New recommendation in FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 34
30	We recommend that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.	Rolled forward from FY 2012	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 35
31	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-00-18-038 Recommendation 36
32	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.	New recommendation in FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 44

33	We recommend that OPM develop and document a security awareness and training strategy tailored to its mission and risk environment.	New recommendation in FY 2017	CLOSED: Closed with issuance of Final Report 4A-CI-00-18-038
34	We recommend that OPM conduct an analysis to identify any resource gaps within its current ISCM program. OPM should use the results of this gap analysis to ensure stakeholders have adequate resources to effectively implement ISCM activities based on OPM's policies and procedures.	New recommendation in FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 46
35	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-00-18-038 Recommendation 47
36	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 35.	New recommendation in FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 48
37	We recommend that the OCIO conduct an agency-wide BIA and incorporate the results into the system-level contingency plans.	New recommendation in FY 2017	OPEN: Rolled forward as Report 4A-CI-00-18-038 Recommendation 50
38	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-00-18-038 Recommendation 51
39	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-00-18-038 Recommendation 52

APPENDIX III

This appendix contains the U.S. Office of Personnel Management's October 1, 2018, response to the draft audit report, issued September 17, 2018.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

October 1, 2018

The Director

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

From: Dr. Jeff T. H. Pon
Director

Subject: Office of Personnel Management Response to the Office of the Inspector General Federal Information Security Modernization Act Audit – FY 2018 (Report No. 4A-CI-00-18-038)

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report for the Federal Information Security Modernization Act (FISMA) Audit for the U.S. Office of Personnel Management (OPM). The OIG comments are valuable to the agency as they afford us an independent assessment of our operations and help guide our improvements to enhance the security of the data furnished to OPM by the Federal workforce, the Federal agencies, our private industry partners, and the public.

While we do not agree with all of the recommendations made in this report, we appreciate OIG's focus on attaining the perfect model of a fully matured, FISMA-compliant cybersecurity program as set forth by the FISMA maturity model and underlying metrics. This year, OPM concurs with 24 of the OIG's 52 recommendations and respectfully non-concurs or partially concurs with the remaining 28 recommendations.

At the outset, OPM emphasizes that it has made great strides over the past year that are not given due credit in the audit report. For instance, we believe that OPM's efforts to develop more robust capabilities to search its systems consistent with past OIG recommendations, and that we discovered, catalogued, or removed dormant legacy software, systems, or hardware demonstrate the hallmarks of Level 4 maturity. However, OIG has reacted to OPM's improved capabilities and processes by downgrading the system Authority area to a material weakness. OPM disputes that the identification and removal of such systems equates to a failure to establish a full system inventory or to utilize an appropriate Authorization process. That OIG would apparently penalize OPM for the success of its corrective efforts which discourages the overall growth and improvement in our system management process.

OPM also notes that a number of the conclusions reached by the OIG in this report appear to be unsubstantiated or reflect a subjective opinion. In some instances, the OIG's comments intrude on the broad discretion afforded to the agency by FISMA to make its own choices regarding appropriate safeguards that are administratively and technologically feasible. The OIG offers comments on OCIO's staffing choices, suggesting that FISMA-related performance standards should be incorporated into performance plans for certain job categories and recommending that OCIO undertake a gap analysis as a top priority to determine appropriate resource and staffing needs. The report reflects OIG's decision to downgrade OPM's security governance structure to a material weakness is largely based on OIG's opinions on OPM staffing decisions. This conclusion ignores the numerous steps that OPM has taken this year to continue to enhance its cybersecurity posture, such as expanded control testing, conducting risk assessments, completion of an agency-wide Business Impact Assessment (BIA), conducting development of the Security Awareness and Training strategy, asset discovery, and better defined system boundaries. OPM does not agree that this area should be downgraded, but will take the OIG's suggestions under advisement and will continue to work with the appropriate personnel within the agency on these topics. In addition, OCIO is committed to appropriate staffing and maintenance of sufficient resources to support OPM's cybersecurity needs. As you will see in our response to several staffing-related recommendations, senior agency leadership is taking steps to help ensure that critical positions within OCIO are funded and allocated. With this support, the agency is actively interviewing candidates for vacant positions within OCIO and has already extended some offers of employment to fill Information System Security Officer (ISSO) and other roles.

Elsewhere, OIG prescribes the use of automated tools, such as in Recommendation 17, where it recommends that OPM implement an automated, enterprise-wide solution for risk tracking and remediation. There is no requirement that OPM employ automated tools, and this recommendation intrudes on OPM's discretion to identify the right tools for its unique needs. Nonetheless, as is discussed in more detail later in this response, OPM agrees that a centralized tool is beneficial and is already well into the process of implementing one.

Finally, OPM and OIG continue to work together toward mutual understanding of the use of the evolving FISMA maturity model and its underlying metrics that were first introduced in Fiscal Year 2017. This year, a new domain area was included in the maturity model that covers Data

Protection and Privacy. OPM recognizes that the report this year will establish a baseline for OPM's future progress in that area and looks forward to further discussion about privacy and its intersection with data security.

Each of the recommendations provided in the draft report is discussed below:

Recommendation 1

We recommend that OPM hire a sufficient number of ISSOs to adequately support all of the agency's major information systems.

Management Response: We concur with the recommendation. The OPM OCIO has conducted an analysis on the funding requirements for ISSO positions and understands where the gaps are. OPM is actively recruiting for these positions, having extended two offers at the end of September and continuing with interviews into early October.

Recommendation 2

We recommend that OPM ensure that OCIO's senior leadership vacancies are filled and that there is a proper separation of duties for assigned roles and responsibilities.

Management Response: We concur with the recommendation. OPM understands the importance of having the individual in the role of the Chief Information Security Officer have information security as his or her primary duties, and will assign an individual to this role in Fiscal Year (FY) 2019.

Recommendation 3

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

Management Response: We do not concur with the recommendation based on the conditions of the recommendation. While OPM agrees with the premise that all active systems in the inventory must have a complete and current authorization, it does not agree with the OIG's conclusion that discovery of assets means that the system inventory and related authorizations are not complete. As referenced by the OIG, significant efforts have been taken by OPM to identify hardware and software assets on its network, including better detection of system boundaries, showing that actions have already been taken that are consistent with past OIG recommendations in this area and that achieve the goal of those recommendation. Issuance of this recommendation along with the supporting language in the report suggests that OPM's posture has worsened, when in fact the work being done in this area clearly shows that OPM has been making strides in the maturity of these programs. Every active system within the inventory has a complete and current authorization and OPM provided to OIG the authorization letters for each system within its system inventory during this annual audit. If systems are identified as a part of OPM's continuous monitoring activities, they will be added to the inventory after completing an assessment and authorization, as appropriate, for that system.

Recommendation 4

We recommend that the performance standards of all OPM system owners be modified to include a requirement related to FISMA compliance for the information systems they own. At a minimum, system owners should be required to ensure that their systems have valid Authorizations.

Management Response: We do not concur with the recommendation. The agency has taken, and will continue to take, OIG's recommendation under advisement and agrees that system owners provide support to the business processes of the agency. However, performance metric adjustments would need input and guidance from the Human Capital Office. Apart from changes to performance standards, OPM will continue to identify appropriate ways to work with system owners to help ensure FISMA compliance. For instance, recently issued cybersecurity policies set forth expectations and requirements for system owners, consistent with NIST 800 Series guidance.

Recommendation 5

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 believes the OIG has provided no basis for determining that the current policy and procedures for defining system boundaries and classifying systems do not contain a sufficient level of detail to be consistently enforced. The OIG simply states that "[t]he current policy and procedures for defining system boundaries and classifying systems does not appear to contain a sufficient level of detail to be consistently enforced." (emphasis added). The agency considers its policy, which is based on NIST guidance and recommendations, to be sufficient and without need of further improvement. Nonetheless, although it is our view that we have fulfilled the requirements of this recommendation, OPM asks the OIG to clarify their rationale on this recommendation.

Recommendation 6

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

Management Response: We concur with the recommendation. Continued updates to centralized tracking, including those that have been released in September, 2018, will improve overall management of the Interconnection Security Agreements (ISAs).

Recommendation 7

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

Management Response: We concur with the recommendation. Continued updates to centralized tracking, including those that have been released in September, 2018, will improve overall management Memorandum of Understandings (MOUs).

Recommendation 8

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

Management Response: We concur with the recommendation. 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 has been at the forefront of working with DHS throughout the lifecycle of the CDM program and will maintain this partnership as CDM continues to evolve. The recommendation here underscores efforts across the Federal government and is not unique to OPM.

Recommendation 9

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

Management Response: We do not concur with the recommendation. While we concur with the general premise of having policies and procedures related to a centralized software inventory, OPM notes that it already has appropriate policies and procedures in place. The OIG states that, "OPM has changed its policy and no longer has a centralized software inventory... " This statement is not correct. OPM issued a Secure Asset Management Policy in January 2018 to reinforce existing asset management requirements and define requirements for management of hardware and software assets. The implementation of a centralized repository for the inventory of these assets is explicitly required by the policy. OPM has also issued an

Information Security Continuous Monitoring Strategy, referenced by the OIG in Section I. The strategy describes the objectives, significant activities, and roles and responsibilities of the continuous monitoring program, which are aligned to the policy.

Further, the OIG report references supplemental guidance from the NIST 800-53, Rev. 4, CM-8 security control in the text related to this recommendation. However, NIST guidance affords agencies significant latitude to determine whether to implement a centralized inventory, and implementation of a centralized inventory is not part of a baseline control per NIST guidance. Therefore, in essence, the OIG's conclusion that there is a deficiency is based on a determination that OPM has not implemented controls that exceed the baseline. Such a conclusion intrudes on matters within the agency's discretion.

Recommendation 10

We recommend that OPM define the standard data elements for an inventory of software assets and licenses with the detailed information necessary for tracking and reporting, and that it update its software inventory to include these standard data elements.

Management Response: We concur with the recommendation. OPM completed the definitions for standard data elements for an inventory of software assets and licenses at the end of August 2018. The standard data elements are provided along with this response. OPM continues to work with DHS on the implementation of the CDM program and will adopt these data elements within its current software asset management capabilities.

Recommendation 11

We recommend that OPM define and communicate a risk management strategy based on the requirements outlined in NIST SP 800-39.

Management Response: We concur with the recommendation. OPM published a Cybersecurity Risk Management Strategy based on the requirements in NIST SP800-39 in September 2018. The Cybersecurity Risk Management Strategy can be provided upon request.

Recommendation 12

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. As stated in the report, a contract was awarded and activities are in progress to develop the enterprise architecture. Despite projected completion dates well into FY 19, we expect that OPM will properly integrate the necessary information security architecture as a part of this process.

Recommendation 13

We recommend that OPM continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, Section 2.3.2 Risk Executive (Function).

Management Response: We partially concur with the recommendation. As described under Recommendation 1 1, OPM published a Cybersecurity Risk Management Strategy based on the requirements in NIST SP800-39 in September 2018. OPM also drafted an Enterprise Risk Management Policy, Enterprise Risk Management Strategy, and an updated charter for the Risk Management Council. OPM expects to finalize and operationalize these documents early in the first quarter of FYI 9. OPM does not concur that the resource limitations described in Section B of the report will impact OPM's ability to develop its Risk Executive Function since those resource limitations are not a part of that function.

Recommendation 14

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

Management Response: We concur with the recommendation. The OCIO will use several processes to remediate this recommendation, including the new Enterprise Project Management Office (PMO), centralized POA&M management tool updates to streamline management of the POA&Ms, and quarterly performance management of POA&M processes.

Recommendation 15

We recommend that OPM update the remediation deadline in its POA&Ms when the control weakness has not been addressed by the originally scheduled deadline (i.e., the POA&M deadline should not reflect a date in the past)

Management Response: We concur with the recommendation. The OCIO will utilize several processes to remediate this recommendation, including the new EPMO, centralized POA&M management tool updates to streamline management of the POA&Ms, and quarterly performance management of POA&M processes.

Recommendation 16

We recommend that OPM complete risk assessments for each major information system that are compliant with NIST guidelines and OPM policy. The results of a complete and comprehensive test of security controls should be incorporated into each risk assessment.

Management Response: We concur with this recommendation. Supported by agency leadership, the OCIO has committed to providing the resources and staffing to properly enforce compliance through ISSOs and the development of an independent assessment team of contractors. The independent assessment team has begun efforts to conduct risk assessments in a consistent manner.

Recommendation 17

We recommend that OPM identify and define the requirements for an automated enterprise-wide solution for tracking risks, remediation efforts, dependencies, risk scores, and management dashboards and implement the automated enterprise-wide solution.

Management Response: We partially concur with the recommendation. OPM recognizes the need for tracking risks to OPM and OPM systems as defined in the OPM Risk Management Strategy; however no federal requirements define the requirement for an automated centralized tool for tracking such risks. Additionally, OPM believes this recommendation may intrude on its discretion to allocate and manage resources in this area. Nonetheless, OPM exercised its broad discretion under FISMA to develop requirements for an automated enterprise-wide solution and will continue to leverage appropriate tools to document and manage risk related to OPM IT systems.

Recommendation 18

We continue to recommend that the OCIO develop a plan and timeline to enforce the new SDLC policy to all of OPM's system development projects.

Management Response: We concur with the recommendation. OPM recognizes the need to enforce its SDLC policy on all IT projects. As referenced by the OIG for this metric, OPM is establishing a new EPMO that will address this recommendation.

Recommendation 19

We recommend that OPM perform a gap analysis to determine the configuration management resource requirements (people, processes, and technology) necessary to effectively implement the agency's CM program.

Management Response: We concur with the recommendation. As referenced by the OIG, OPM has already dedicated resources to establishing a new EPMO. Defining the resource requirements to effectively implement the configuration management program is one of the objectives of the effort.

Recommendation 20

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. OPM is in the process of establishing a new EPMO that will significantly modify its configuration management practices and create new planning tools. Given the transformation already underway in this area that will incorporate best practices based on lessons learned and other factors, OPM does not agree that this recommendation is timely or appropriate.

Recommendation 21

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. OPM is establishing a new EPMO that will address this recommendation.

Recommendation 22

We recommend that the OCIO conduct routine compliance scans against established baseline configurations for all OPM information systems. This recommendation cannot be addressed until Recommendation 21 has been implemented.

Management Response: We concur with this recommendation. OPM is establishing a new EPMO that will address this recommendation.

Recommendation 23

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. OPM plans to expand and implement standard security configurations for all servers and databases.

Recommendation 24

We recommend that the OCIO conduct routine compliance scans against [the standard security configuration settings] for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 23 has been completed.

Management Response: We do not concur with the recommendation. The OCIO is currently conducting scans of OPM servers and databases. OCIO will continue the practice for any new security standards that we introduce or implement. The practice that OPM currently has in place is working appropriately and is consistent with security standards.

Recommendation 25

For OPM configuration standards that are based on a pre-existing generic standard, we recommend that OPM document all instances where the OPM-specific standard deviates from the recommended configuration setting.

Management Response: We concur with the recommendation. Increased ISSO resources will allow for expanded documentation and approval of deviations.

Recommendation 26

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

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

Recommendation 27

We recommend that the OCIO implement a process for updating and maintaining credentials for its scanning accounts.

Management Response: We do not concur with this recommendation because OCIO has already implemented a process for updating and maintaining credentials for its scanning accounts and provided information to reflect that implementation to the OIG in May 2018.

Implementation occurred immediately following the conclusion of the prior year FISMA audit in response to the issuance of Recommendation 23 from the OIG Report 4A-CI-00-17-020.

Recommendation 28

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 do not concur with this recommendation. As described under our response to Recommendation 27, OPM implemented a process for updating and maintaining credentials for its scanning accounts and provided information to reflect that implementation to the OIG in May 2018. Implementation occurred immediately following the conclusion of the prior year FISMA audit in response to the issuance of Recommendation 23 from the OIG Report 4A-C1-OO-17-020.

Recommendation 29

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 partially concur with the recommendation. OPM understands we have unsupported software and operating systems; however, risk assessments and mitigating controls have been implemented by the agency so that detected vulnerabilities cannot be exploited. Additionally, projects are underway to remove unsupported software and systems from the network.

Recommendation 30

We recommend that the OCIO implement a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.

Management Response: We do not concur with the recommendation because OPM has already implemented this type of process. The OIG states in the report that OPM does not have a process to record or track the remediation status for other routine security weaknesses identified during vulnerability scans. However, in February 2018, OPM developed a process for tracking the remediation status of weaknesses identified during vulnerability scans in response to the prior year audit. OPM intends to use this process until the DHS CDM program delivers automated data feeds to OPM's tracking repository.

Recommendation 31

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

Management Response: We partially concur with the recommendation. The agency has a process for patch management to help ensure timely deployment of patches and has seen significant improvements in timeliness and an ability to routinize patch deployments over the past year. OCIO expects further improvements in timeliness over the upcoming year and will utilize enterprise change management processes. This change management process will include submissions of evidence supporting adherence to the processes. In the short term, a patch management tiger team plan is in draft form.

Recommendation 32

We recommend that OPM conduct an analysis to identify limitations in the current ICAM program in order to ensure that stakeholders have adequate resources (people, processes, and technology) to implement the agency's ICAM activities.

Management Response: We partially concur with this recommendation. The agency does not consider ICAM to be a distinct program, though it could potentially be deemed a service area under the Security Operations Center Monitoring and Analysis team. The agency has initial plans on how to address this recommendation that can be incorporated as part of a long term strategy.

Further, the OIG references the loss of ISSOs as a reason for the lack of implementation of ICAM controls but does not explain the connection it has made between ISSO resourcing and the perceived limitations in the ICAM program. It is difficult for OPM to assess its response to this recommendation without further information.

Recommendation 33

We recommend that OPM develop and implement an ICAM strategy that considers a review of current practices ("as-is" assessment) and the identification of gaps (from a desired or "to-be" state), and contains milestones for how the agency plans to align with Federal ICAM initiatives.

Management Response: We partially concur with this recommendation. The agency does not consider ICAM to be a distinct program though it could potentially be deemed a service area under the Security Operations Center Monitoring and Analysis team. The agency has initial plans on how to address this recommendation that can be incorporated as part of a long term strategy.

Recommendation 34

We recommend that OPM implement a process to capture and share lessons learned on the effectiveness of its ICAM policies, procedures, and processes to update the program.

Management Response: We partially concur with this recommendation. The agency does not consider ICAM to be a distinct program though it could potentially be deemed a service area under the Security Operations Center Monitoring and Analysis team. The agency has initial plans on how to address this recommendation that can be incorporated as part of a long term strategy.

Recommendation 3 5

We recommend that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.

Management Response: We concur with the recommendation. The OCIO has plans to deploy an identity and access tool to assist with meeting OMB M-11-11.

Recommendation 36

We recommend that 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 policy requirements into tool deployment. Use of this tool will also aid in auditing of user accounts.

Recommendation 37

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

Management Response: We partially concur. We agree that in order for the privacy program to develop into a more robust program, additional resources along with more clearly articulated roles and responsibilities are needed, both in the office that has immediate responsibility for privacy matters and throughout OPM. We disagree that no roles and responsibilities for privacy are currently defined at OPM. OPM elevated the Chief Privacy Officer/Senior Agency Official for Privacy to a senior-level position reporting directly to the Director of OPM. That position, based on the position description and the requirements set forth in guidance from the Office of Management and Budget, has responsibility for privacy policy and compliance at OPM.

Recommendation 38

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

Management Response: We partially concur. We agree that a more focused articulation of privacy policies and procedures that are separate from and/or integrated with information security policy and procedures, as appropriate, will be beneficial and we are working towards that end. We disagree that there are not currently in place plans, policies, and procedures for the protection of PII. The Information Security and Privacy Policy Handbook includes appropriate privacy provisions, as do the current PIA and SORN guides. In addition, the Chief Privacy Officer implemented a robust template for Privacy Impact Assessments (PIA) that has been in use since calendar year 2017, as well as a new template for Privacy Threshold Analyses (PTA). The PTA template has been implemented both to determine the need for a PIA or a Privacy Act system of records notice and to track appropriate privacy controls as articulated in NIST 800-53, Appendix J. In addition to those OPM-specific policies and procedures, the agency continues to rely on overarching privacy guidance issued by the Office of Management and Budget and NIST.

Recommendation 39

We recommend that OPM implement controls over encryption of data at rest on its IT systems.

Management Response: We do not concur with this recommendation. OPM has implemented controls over encryption of data at rest on its IT systems. The OIG has not yet provided OPM with a clear understanding of what evidence is needed to demonstrate that controls over encryption of data at rest on its IT systems are in place.

Recommendation 40

We recommend that OPM implement controls over encryption of data in transit on its IT systems.

Management Response: We do not concur with this recommendation. OPM has implemented controls over encryption of data in transit on its IT systems. The OIG has not yet provided OPM with a clear understanding of what evidence is needed to demonstrate that controls over encryption of data at rest on its IT systems are in place.

Recommendation 41

We recommend that OPM develop and implement policies and procedures related to data exfiltration and enhanced network defenses.

Management Response: We do not concur with this recommendation. OPM has issued several policies covering the data exfiltration and enhanced network defenses, including: 1) Information System Monitoring; 2), OPM Boundary Protection; 3) OPM Malicious Code; and 4) Mobile Code.

Recommendation 42

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

Management Response: We partially concur. We agree that an annual table top exercise to review the Breach Response Plan can help clarify and refine roles and responsibilities in the event of a breach and help to more clearly articulate the appropriate risk analysis and mitigation steps that should be taken, as provided by the Breach Response Plan and OMB Memorandum 17-12. We disagree with the OIG's underlying premise that not conducting a table top exercise has increased OPM's risk of major data loss in the event of a security incident. Annual security and privacy awareness training informs the OPM workforce of when to report a loss or potential loss of PII to the Security Operations Center (SOC). The SOC routinely informs appropriate OPM personnel when an incident has occurred and steps are taken to address and mitigate any potential harm as appropriate. The Chief Privacy Officer is also a part of the senior members of the OPM staff that routinely meets and interacts with other key members of the workforce, which allows for consistent communication regarding the protection of sensitive identifiable information to occur.

Recommendation 43

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. We agree that appropriate annual privacy training should be provided. This is done formally through the annual security and privacy awareness training that all individuals at OPM are required to complete. We also agree that it would be beneficial to evaluate more formally whether there are individuals who, given their job responsibilities and exposure to PII, should receive any additional annual training. We disagree with the underlying assumption that individuals who regularly handle PII will always require specialized formal annual training. In many instances the annual awareness training, followed by tailored discussions with various offices, can be just as effective. To date, the Chief Privacy Officer has provided presentations on privacy and engaged in group discussions with various offices in an effort to further provide appropriate privacy awareness and compliance.

Recommendation 44

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

Management Response: We concur with this recommendation. OPM completed the assessment of its workforce's knowledge, skills, and abilities in accordance with the instructions given for the Federal Cybersecurity Workforce Assessment Act of 2015. This assessment was completed in August 2018, after the OIG audit testing period, and can be provided upon request.

Recommendation 45

We recommend that OPM develop and document a security awareness and training strategy tailored to its mission and risk environment.

Management Response: We do not concur with this recommendation. The Security Awareness and Training Strategy was completed in May 2018 and was delivered to the OIG in June 2018. OPM's view is that the strategy is appropriately tailored to the agency mission and risk environment.

Recommendation 46

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

Management Response: We partially concur with this recommendation. OPM agrees that challenges in resources have affected the ISCM program. OPM has identified needs and have responded by recruiting and making plans to bring onboard additional personnel.

Recommendation 47

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

Management Response: We concur with this recommendation. OPM agrees that challenges in resources have affected annual control testing. Additional resources joining the OCIO in the near future will help to ensure thorough annual security control testing for all systems.

Recommendation 48

We recommend that OPM evaluate qualitative and quantitative performance measures on the performance of its ISCM program once it can consistently acquire security assessment results, as referenced in recommendation 47.

Management Response: We do not concur with this recommendation. Performance measures for the ISCM program have been established and the OCIO is conducting an evaluation of the management of POA&Ms and inventory management. The use of a centralized tool is expected to provide a significantly expanded capability for evaluation.

Recommendation 49

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

Management Response: We do not concur with the recommendation. The OCIO is aware of the technology and resource gaps related to enterprise disaster recovery testing that can result in an ability to further plan development and conduct exercises and is taking steps, supported by agency leadership, to eliminate those gaps. The OIG cites ISSO staffing issues as reason for contingency plan development and testing weaknesses but does not explain how it has reached this conclusion.

Recommendation 50

We recommend that the OCIO conduct an agency-wide BIA and incorporate the results into the system-level contingency plans.

Management Response: We do not concur with the recommendation. OPM completed an agency-wide BIA and developed a new template with instructions for incorporating the results into system-level contingency plans in May 2018. The document can be provided upon request.

Recommendation 51

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

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

Recommendation 52

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

Management Response: We concur with the recommendation. The OCIO will coordinate with each system's Program Management Office (PMO) including the System Owners and

Authorizing officials to help ensure annual testing of the contingency plans in accordance with policy.

Technical Comments on General Federal Information Security Modernization Act Audit — FY 2018 (Report No. 4A-C1-OO-18-038), dated September 17, 2018

- Scope and Methodology, page 4, outlines that the criteria used in conducting the audit included OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information. OMB M-07-16 was rescinded on January 3, 2017, by OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information.

- Section G. Data Protection and Privacy, page 33, states that OPM's privacy program is supported, in part, by intermittent supporting contract staff. That is not accurate. The Chief Privacy Officer does not have any contract staff support and is currently supported by two detailees from the OCIO's Information Management Office.

Again, thank you for the opportunity to provide comment. Please contact Mr. David Garcia or me if you have question or need additional information.

cc:

Michael D. Dovilla
Chief of Staff

Stephen Billy
Deputy Chief of Staff

David A. Garcia
Chief Information Officer

Kathleen M. McGettigan
Chief Management Officer

Dennis D. Coleman
Chief Financial Officer

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

Janet L. Barnes
Director, Internal Oversight and Compliance

Jeffrey P. Wagner
Associate Chief Information Officer for Infrastructure

Kathie A. Whipple
Acting General Counsel

Robert M. Leahy
Deputy CIO

Kellie Cosgrove Riley
Chief Privacy Officer

Norbert Vint
Acting Inspector General

Michael R. Esser
Assistant Inspector General for Audits

[redacted]
Auditor-in-Charge, Office of the Inspector General

Anthony C. Marucci
Director, Office of Communications

Jonathan J. Blyth
Director, Congressional, Legislative & Intergovernmental Affairs

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