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 2017

Report Number 4A-CI-00-17-020
October 27, 2017

EXECUTIVE SUMMARY

Federal Information Security Modernization Act Audit Fiscal Year 2017

Report No. 4A-CI-00-17-020 **October 27, 2017**

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 2017 at OPM headquarters in Washington, D.C.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

The Fiscal Year (FY) 2017 FISMA Inspector General reporting metrics fully adopted a maturity model evaluation system derived from the National Institute of Standards and Technology's Cybersecurity Framework. The Cybersecurity Framework is comprised of seven "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 2017, OPM's cybersecurity maturity level is measured as "2 - Defined."

Our audit also determined that OPM has made improvements in its Security Assessment and Authorization (Authorization) program. We upgraded the previous material weakness related to Authorizations to a significant deficiency for FY 2017 based on OPM's "Authorization Sprint" and the agency's continued efforts to maintain Authorizations for all information systems.

However, we once again identified a significant deficiency in OPM's information security management structure. OPM is not making substantial progress in implementing our FISMA recommendations from prior audits. While resource limitations certainly impact the effectiveness of OPM's cybersecurity program, the staff currently in place is not fulfilling its responsibilities that are outlined in OPM policies and required by FISMA.

The sections below provide a high level outline of OPM's performance in each of the five cybersecurity framework functions:

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.

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

Authorization	**Security Assessment and Authorization**
BIA	**Business Impact Analysis**
CBIS	**Consolidated Business Information System**
CDM	**Continuous Diagnostics Mitigation**
CIGIE	**Council of Inspectors General on Integrity and Efficiency**
CISO	**Chief Information Security Officer**
CM	**Configuration Management**
CSP	**Cybersecurity Program**
DHS	**U.S. Department of Homeland Security**
FFS	**Federal Financial System**
FICAM	**Federal Identity, Credential, and Access Management**
FIPS	**Federal Information Processing Standards**
FISCAM	**Federal Information System Controls Audit Manual**
FISMA	**Federal Information Security Modernization Act**
FY	**Fiscal Year**
ICAM	**Identity, Credential, and Access Management**
IG	**Inspector General**
ISA	**Interconnection Security Agreement**
ISCM	**Information Security Continuous Monitoring**
ISSO	**Information System Security Officer**
IT	**Information Technology**
LACS	**Logical Access Control Systems**
MOU/A	**Memorandum of Understanding/Agreement**
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**
PIV	**Personal Identity Verification**
POA&M	**Plan of Action and Milestones**
SDLC	**Systems Development Lifecycle**
SharePoint	**Microsoft's SharePoint Software**
SP	**Special Publication**
TIC	**Trusted Internet Connections**

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) 2017 IG FISMA Reporting Metrics. 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 2017 metrics also mark a continuation of the work that OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) undertook in FY 2015 and FY 2016 to move the IG assessments toward a maturity model approach. In previous years, CIGIE, 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 2017 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;
- 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 OPM's major information systems – the implementation of Microsoft's SharePoint software (SharePoint), the Federal Financial System (FFS), and the Consolidated Business Information System (CBIS).

SCOPE AND METHODOLOGY

We conducted this performance audit in accordance with 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 2017.

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 SharePoint, FFS, and CBIS 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:

- FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics;
- OPM Information Security and Privacy Policy Handbook;
- 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 – Policy for a Common Identification Standard for Federal Employees and Contractors;

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

- Federal Information Processing Standards (FIPS) 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 (FICAM) Roadmap Implementation Guidance;
- FIPS 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 2017 in OPM's Washington, D.C. office.

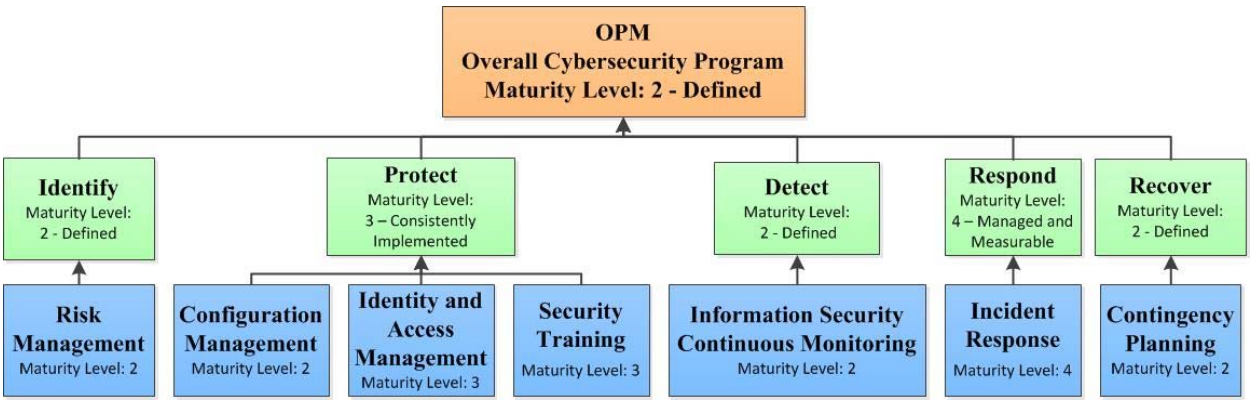
COMPLIANCE WITH LAWS AND REGULATIONS

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

In FY 2017, the FISMA IG Reporting Metrics fully adopted a maturity model evaluation system derived from the NIST Cybersecurity Framework. The Cybersecurity Framework is comprised of five "function" areas that are mapped to seven "domains" that fall under each function area. These seven 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 through 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):

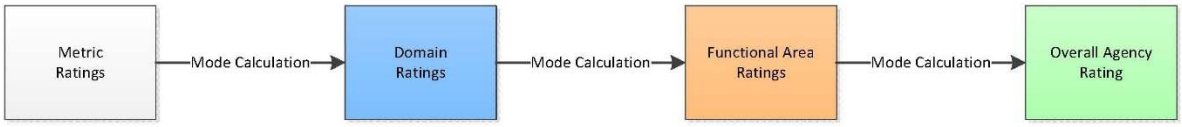


The following table outlines the description of each maturity level rating, as defined by the FY 2017 IG FISMA Reporting Metrics:

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) of each individual metric is used to calculate the domain rating. Similarly, the mode of the domain ratings is used to assign the function area rating. The overall agency rating is calculated by the same methodology.



The remaining sections of this report provide the detailed results of our audit. Sections B and C (Information Security Governance and Security Assessment and Authorizations, respectively) do not directly map to the FY 2017 IG FISMA Reporting Metrics. However, both areas represent significant deficiencies in the agency's IT security program and warrant discussion in this report. Sections D through J outline how we rated the maturity level of each individual metric, which ultimately determined the agency's maturity level for each domain and function.

B. 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.

Our FISMA audit reports from FY 2007 through FY 2013 reported this issue as a material weakness, and our recommendation was that the agency recruit a staff of information security professionals to act as Information System Security Officers (ISSO) that report to the OCIO.

OPM has since centralized its cybersecurity program under a Chief Information Security Officer (CISO) supported by a team of ISSOs. This team has developed policies and procedures

designed to improve the efficiency in which it operates, and has implemented a variety of technical security tools and controls that help protect the agency from cyber-attack.

We believe that this centralized security governance structure *can* be effective. However, the CISO organization continues to struggle in implementing long-standing cybersecurity controls required by FISMA. Specifically, in FY 2017 OPM again scored poorly in FISMA metrics related to continuous monitoring (see section H), Plan of Action and Milestones (POA&M) management (see section D), and contingency planning (see section J). There are audit recommendations in these sections that are over a decade old. Historically, when OPM makes progress in one cybersecurity domain, it does so at the expense of another. For instance, this year significant resources were dedicated to improving OPM's Authorization process, but there was notable regression in other domains.

OPM is not making substantial progress in implementing prior OIG FISMA recommendations.

In addition, OPM is not making substantial progress in implementing our FISMA recommendations from prior audits. OPM has only closed 34 percent of the FISMA findings issued in the past two years, and we expect the number of new recommendations issued to significantly increase as the FISMA audits continue to evolve and look into new areas of the agency's technical operations.

We would also like to directly address comments that OPM made in its response to our draft audit report that imply that OIG audits contribute to the inefficiencies of the agency's cybersecurity program. OPM cited "audit fatigue" as one of the factors leading to its inability to execute its mission and address cybersecurity related audit findings and recommendations. Although we agree that audits can be a strain on resources, we believe that the primary cause of OPM's "audit fatigue" is the OCIO staff's inability to maintain complete, detailed, and organized documentation. OPM's concerns about "overlapping and duplicative" audit requests can be directly tied to the agency's inability to respond to the original requests in a complete and timely manner. This requires the auditors to issue additional requests for the same information, placing an undue burden on both parties.

An example of this inefficiency occurred during the FY 2017 audit of OPM's Authorization process. OIG auditors spent many weeks auditing the Authorization package for one of OPM's major general support systems, only to discover that the OCIO had provided an outdated, inaccurate version. As a result, we wasted over 600 hours auditing useless and irrelevant information.

Throughout this current FISMA audit, the OCIO was also extremely inefficient in its management of audit interviews. The OIG provided OPM with detailed lists of interview topics and requested that the OCIO schedule meetings with the appropriate subject matter experts. However, there were many instances where the OCIO did not invite the correct individuals to meetings and/or did not share the detailed list of topics to be covered with the attendees, greatly reducing the efficiency of the interview process.

The annual FISMA reporting metrics are publicly available documents, and are made available to OPM and the OIG at the same time, and are generally covering the same topics every year. It would seem obvious that the OCIO should anticipate the required documentation and interview requests and stage the information in a readily accessible location. This audit is essentially an "open book test," but, inexplicably, OPM continues to struggle in providing timely documentation and appears to be generally unprepared to respond to routine audit requests.

While resource limitations certainly impact the effectiveness of OPM's cybersecurity program, the staff currently in place is not fulfilling its responsibilities outlined in OPM policy and required by FISMA. We continue to find issues with the quality of the work that is completed, and routinely detect instances where work was completed that did not adhere to OPM policy.

Although OPM's cybersecurity posture is notably better than it was in the past, **we believe that OPM's security governance structure continues to represent a significant deficiency in the agency's internal controls**.

Failure to have sufficient, well qualified, and well organized resources in place to manage a cybersecurity program increases the risk that the program will not operate as intended and that critical control requirements will not be met.

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

Recommendation 1 (Rolled forward from 2016)

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

OPM Response:

"We concur with the recommendation. As discussed above, OCIO's resources have been impacted by budgetary uncertainties and the ensuing difficulties in planning and funding hiring actions in upcoming fiscal years. OPM faces challenges in its ability to prioritize cybersecurity positions over other agency hiring decisions. A gap also exists in OPM's ability

to retain and backfill cybersecurity positions. The Agency priorities may not always align with the cybersecurity priorities. Additionally, OPM Cybersecurity has had challenges restructuring its organization to better assign supervisors and team leads within the Cybersecurity Program [(CSP)] and anticipates that restructuring will enhance CSP's capabilities to address concerns the OIG raises, including enhancing CSP's ability to manage new policies and develop improved quality control mechanisms."

OIG Comment:

As part of the audit resolution process, we recommend that the OCIO provide OPM's office of Internal Oversight and Compliance 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.

C. SECURITY ASSESSMENT AND AUTHORIZATION

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.

Previous FISMA audits identified a material weakness in OPM's Authorization process related to incomplete, inconsistent, and sub-par work products. OPM resolved the issues by implementing new policies and procedures to standardize the Authorization process. However, throughout FY 2014 and FY 2015, the number of OPM systems without a current and valid Authorization significantly increased, and we reinstated the material weakness related to this issue in our FY 2015 FISMA audit.

In April 2015, OPM's OCIO issued a memorandum that granted an extension of the previous Authorizations for all systems whose Authorization had already expired, and for those scheduled to expire through September 2016. The justification was that OPM was in the process of modernizing its IT infrastructure and that once this modernization was completed, all systems would have to receive new Authorizations anyway. We expressed serious concern with this approach, and warned the agency of the extreme risk associated with neglecting the IT security controls of its information systems.

In an effort to revitalize its Authorization program, in FY 2016 OPM initiated an "Authorization Sprint" designed to get all of the agency's systems compliant with the Authorization

requirements. OPM dedicated significant resources toward re-Authorizing the systems neglected because of the 2015 Authorization moratorium.

By the third quarter of FY 2017, the agency had a valid Authorization in place for 80 percent of the agency's major information systems, including the critical Local Area Network / Wide Area Network general support system. The OCIO has also successfully addressed some of the critical Authorization-related weaknesses that our audits had identified. **As a result of these improvements, we are upgrading the material weakness related to system Authorizations to a significant deficiency**. There are still widespread issues – albeit less severe – in OPM's Authorization packages. These ongoing issues primarily relate to documentation inconsistencies and the incomplete or inadequate independent testing of the systems' security controls.

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 H, Information Security Continuous Monitoring).

The lack of an Authorization can indicate that security controls are not operating effectively or that there are unacceptable levels of risk in a system.

Recommendation 2 (Rolled forward from 2014)

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

OPM Response:

"We partially concur with the recommendation. The OIG states in the report that 80% of OPM's information systems had a valid authorization by Q3, FY 2017; however all OPM information systems held a valid authorization in early Q2, FY 2017. The OIG states in its report that there are documentation inconsistencies and incomplete or inadequate independent testing of the system security controls that need to be addressed. In FY 2017, OPM recognized areas where there are inconsistencies in documentation or further independent testing of security controls would be beneficial. After the Cybersecurity program is restructured and clarification on resources is provided, we anticipate additional improvements in the quality and consistency of the [authorization to operate] packages through improved management and oversight."

OIG Comment:

As of the end of the fiscal year (and as of the date of this report) OPM operated production systems that had not been subject to a complete and current Authorization. The recommendation and the narrative supporting it are still applicable, and the recommendation remains open.

Recommendation 3 (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. However, consultation with the subject matter experts within the Agency to determine whether and how to implement this recommendation is necessary and appropriate."

OIG Comment:

Although OPM disagrees with this recommendation, OCIO officials intend to consult with subject matter experts within the agency to determine how and whether to implement the recommendation. Therefore, it appears that the agency has not yet determined whether it agrees with the recommendation. We will provide additional feedback once OPM solidifies its position.

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 "2 – Defined."**

Metric 1 – Inventory of Major Systems and System Interconnections

FY 2017 Maturity Level: 2 – Defined. OPM has defined the policies and procedures for managing its inventory of systems and its interconnections.[1] OPM maintains a repository for documenting its system inventories and system interconnections. The inventory includes all major information systems, but not all of the system interconnections.

NIST SP 800-53, Revision 4, requires that 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 system interconnections increases the risk that information systems will improperly share or fail to protect sensitive information.

Recommendation 4 (Rolled forward from 2014)

We recommend that the OCIO ensure that all ISAs are valid and properly maintained.

OPM Response:

"We concur with the recommendation. An audit of VPN connections has been completed and an audit of firewall connections will be completed next in order to complete mapping of connections. OPM is putting new policies and quality assurance mechanisms in place so that all ISAs will be valid and properly maintained."

Recommendation 5 (Rolled forward from 2014)

We recommend that the OCIO ensure that a valid MOU/A exists for every interconnection.

OPM Response:

"We concur with the recommendation. OPM is putting new [policies] and quality assurance mechanisms in place to improve visibility and review of all interconnection MOU/As exist for each interconnection."

[1] System interconnections are documented in memorandum of understanding/agreements (MOU/A) and interconnection security agreements (ISA).

Metric 2 – Hardware Inventory

FY 2017 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 6 (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 and DHS Continuous Diagnostics and Mitigation (CDM) have implemented a solution for correlating these elements to FISMA system boundaries. Implementation progress has been limited due to the lack of system documentation available to identify servers and tie them to their systems. Efforts are underway to complete server system tagging to facilitate this effort."

Metric 3 – Software Inventory

FY 2017 Maturity Level: 1 – Ad-hoc. OPM uses a software tool to maintain its centralized software inventory. The inventory has some standard data elements (e.g., name, owner, and description) but does not contain the level of detail necessary for thorough tracking and reporting (e.g., vendor, version, installation locations, license information, and information system association).

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 include the necessary information in a software inventory increases the risk that the agency will not fully understand the information assets in its environment.

Recommendation 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.

OPM Response:

"We concur with the recommendation. OPM and DHS CDM have implemented a solution for correlating these elements to FISMA system boundaries. Implementation progress has been limited due to the lack of system documentation available to identify software. Efforts are underway to complete a white/black list of enterprise software to facilitate this effort."

Metric 4 – System Security Categorization

FY 2017 Maturity Level: 3 – Consistently Implemented. OPM has implemented policies and procedures for categorizing its information and information systems that follow FIPS 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

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

FY 2017 Maturity Level: 1 – Ad-hoc. OPM has defined policies for risk management and recently created a Risk Management Council. The council serves as the risk executive function at OPM and develops the agency-wide risk management approach and guidance. The council has begun to meet regularly and has defined a risk profile for OPM, but has not yet established an overall risk strategy for the agency.

A risk management strategy provides the guidance for understanding, tracking and remediating risks and making risk-based decisions for agency systems and resources.

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 8

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. Through its Risk Management Council, OPM plans to develop the agency's Enterprise Risk Management Framework and Policy during FY 2018. This will define the agency's risk management strategy."

Metric 6 – Information Security Architecture

FY 2017 Maturity Level: 1 – Ad-hoc. OMB's Federal Enterprise Architecture Guidance states that "Enterprise architecture is a management best practice for aligning business and technology resources to achieve strategic outcomes, improve organizational performance and guide Federal agencies to better execute their core missions. An enterprise architecture also describes the current and future state of the agency, and lays out a plan for transitioning from the current state to the desired future state."

OPM's enterprise architecture has not been updated since 2008, and it does not support the necessary integration of an information security architecture. 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." OPM's IT environment has undergone significant changes since 2008, and while the agency has started to develop an information security architecture, it cannot complete the information security architecture without updating its enterprise architecture.

NIST SP 800-53, Revision 4, requires that "The information security architecture includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface." 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 9

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. OPM plans to make appropriate updates to its Enterprise Architecture to include relevant information security architecture elements."

Metric 7 – Risk Management Roles, Responsibilities, and Resources

FY 2017 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 newly created Risk Management Council, and defining the responsibilities of information system owners, information security staff, and authorizing officials. As mentioned above, the council has started to fulfill its role in overseeing the risk management program with the creation of the risk profile, but is not yet fulfilling all of the responsibilities of the risk executive function required by NIST. In addition, the resource limitations noted above in Section B, Information Security Governance, also negatively impact the risk management program, since the CISO organization plays a key role in tracking 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 10 (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 concur with the recommendation. During FY 2018, as OPM matures it Enterprise Risk Management Program, we will take into account the requirements related to the Risk Executive Function outlined in NIST SP 800-39."

Metric 8 – Plan of Action and Milestones

FY 2017 Maturity Level: 2 – Defined. The 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 the fact that system owners were not meeting the self-assigned scheduled completion dates for remediating weaknesses.

This year OPM has made efforts to improve its POA&M process. In March, the OCIO released an updated POA&M policy that details the POA&M process and the roles and responsibilities of those involved. In addition, OPM has started using a new tracking tool for its POA&M repository.

Over 96 percent of POA&Ms are more than 30 days overdue.

However, the 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, over 96 percent of POA&Ms were more than 30 days overdue,

and over 88 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. As discussed in section B, above, 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 significant deficiency 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 11 (Rolled forward from 2016)

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

OPM Response:

"We concur with the recommendation. In FY 2017, OPM introduced a new management process for reviewing POA&M content, including milestones and remediation dates for POA&Ms. OPM will continue to improve the process to support better milestone definition, identification of remediation dates, and POA&M reviews and updates."

Recommendation 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).

OPM Response:

"We concur with the recommendation. In FY 2017, OPM introduced a new management process for reviewing POA&M content, including milestones and remediation dates for POA&Ms. OPM will continue to improve the process to support better milestone definition, identification of remediation dates, and POA&M reviews and updates."

Metric 9 – System Level Risk Assessments

FY 2017 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 have its controls assessed for risk on a routine basis as part of the Authorization process. We reviewed a sample of risk assessments for systems that were authorized in FY 2017, and noted that a majority had issues 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 to operate.

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 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.

OPM Response:

"We concur with this recommendation. The resource, budget, staffing, alignment challenges identified above impact CSP's ability to properly enforce compliance through ISSOs. Our work to address those issues, and restructure the office will better enable CSP to address this recommendation."

Metric 10 – Risk Communication

FY 2017 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. 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 2017 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 2017 Maturity Level: 1 – Ad-hoc. OPM does not have a centralized system or tool to view enterprise-wide risk information, nor has it defined requirements to develop one. 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 agency-wide risk information in a centralized location.

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 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.

OPM Response:

"We concur with the recommendation. OPM plans to explore options for an automated enterprise-wide risk management solution during FY 2018. However, acquisition of an automated tool will be subject to the availability of resources."

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

As noted in the FY 2016 OIG FISMA audit report, OPM has a long history of troubled system development projects. At the end of FY 2013, the OCIO published a new Systems Development Lifecycle (SDLC) policy, which was a significant first step in implementing a centralized SDLC methodology at OPM. The new SDLC policy incorporated several prior OIG recommendations related to a centralized review process of system development projects. However, this SDLC has not been actively enforced for all IT projects in the Agency.

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

In FY 2016, the Agency's enormous IT infrastructure overhaul initiative was scrapped and divided into multiple parallel efforts to consolidate and modernize OPM's IT infrastructure. While our concerns with the Agency's infrastructure improvement project are reported separately from our FISMA audits, we have ongoing concerns that OPM's failure to follow a comprehensive SDLC will result in information systems not being properly managed throughout the lifecycle and that new projects will fail to meet the stated objectives, timelines, and budgets.

OCIO's response to a prior year audit recommendation related to SDLC discussed the creation of another SDLC policy. However, we still look to see that a comprehensive SDLC is enforced for all of OPM's system development projects.

The Federal Information System Controls Audit Manual (FISCAM) guidance states that "The SDLC should provide a structured approach for identifying and documenting needed changes to computerized operations; assessing the costs and benefits of various options, including the

feasibility of using off-the-shelf software; and designing, developing, testing, and approving new systems and system modifications."

The lack of an effective SDLC methodology increases the risk that OPM will waste resources (time and money) in 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 15 (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 plans to update the SDLC by elevating best practices and lessons learned from IT PMOs engaged in Agile development. The new SDLC will also leverage recommendations from engagement with 18F to ensure OCIO benefits from recognized industry standards and processes along with practical first-hand experience. OPM will develop a plan and timeline to implement and enforce the updated SDLC policy."

E. CONFIGURATION MANAGEMENT

Configuration Management (CM) controls allow an organization to establish information system configuration baselines, processes for securely managing changes to configurable settings, and procedures for monitoring system software. While OPM has made improvements in some elements of its CM program, we identified multiple weaknesses in this area. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Configuration Management domain is "2 – Defined."**

Metric 14 – Configuration Management Roles, Responsibilities, and Resources

FY 2017 Maturity Level: 2 – Defined. OPM has policies and procedures in place defining CM stakeholders and their roles and responsibilities. However, OPM has indicated that it does not currently have adequate resources (people, processes, and technology) to effectively manage its 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 ensuring that its stakeholders have identified the required resources to manage CM operations, the agency increases the likelihood that improperly configured devices exist within its network and therefore increases the threat of malicious attacks that could exploit these weaknesses.

Recommendation 16

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

OPM Response:

"We concur with the recommendation. OPM plans to conduct an analysis to better determine CM resource requirements."

Metric 15 – Configuration Management Plan

FY 2017 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. 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 17

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

OPM Response:

"We partially concur with this recommendation. OPM concurs with the recommendation to document lessons learned and update its configuration management plan. However, OPM has implemented processes and procedures to document and communicate risks identified through configuration management activities to Authorizing Officials. This process is defined in artifacts provided during the audit. OPM will work with the OIG to provide clarification, where needed."

OIG Comment:

After reviewing the provided documentation the OIG agrees that there is a process in place to communicate the risks to stakeholders when identified through configuration management activities. However, this does not upgrade OPM's rating for this metric and we continue to recommend that OPM document its lessons learned from configuration management activities and update its configuration management plan as appropriate and provide evidence to OPM's Internal Oversight and Compliance office when they have implemented this recommendation.

Metric 16 – Implementation of Policies and Procedures

FY 2017 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:

- Establish and maintain baseline configurations and inventories of information systems;
- Routinely verify that information systems are actually configured in accordance with baseline configurations; and
- Conduct routine vulnerability scans on all information systems and remediate any vulnerabilities identified from the scan results in a timely manner.

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

Metric 17 – Baseline Configurations

FY 2017 Maturity Level: 1 – Ad-Hoc. OPM has not developed a baseline configuration for all of its information systems. NIST SP 800-53, Revision 4, states that "Baseline configurations are

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

OPM has not established baseline configurations for all of its information systems, and therefore is unable to effectively audit its system configurations.

OPM routinely runs compliance scans on its information systems to ensure that no system is modified outside of the approved change control process. However, OPM does not currently run scans to verify that information systems (i.e., the elements listed above in the NIST definition of a baseline configuration) 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, 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 the agency's policies and leaves them vulnerable to malicious attacks that exploit those misconfigurations.

Recommendation 18

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. OCIO plans to work with system owners across OPM to establish baseline configuration that will be kept under configuration control."

Recommendation 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.

OPM Response:

"We concur with this recommendation. Currently OCIO performs compliance scans based on security configuration standards in compliance with OPM policy. Scans will be updated to align with approved architecture baselines and reports will be submitted to Authorizing Officials as part of the continuous monitoring process."

Metric 18 – Security Configuration Settings

FY 2017 Maturity Level: 1 – Ad-Hoc. In FY 2014, we issued a recommendation that OPM establish baseline configurations for all of its operating platforms based on the OIG FISMA metrics at the time. However, in FY 2017, the OIG FISMA metrics now distinguish the requirements of implementing baseline configurations from implementing standard security configuration settings. As such, we have changed the terminology in our reports to reflect this change.

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."

OPM currently leverages several common best-practice configuration setting standards for its information systems. However, OPM has not documented a standard security configuration setting for all of its operating platforms and has not tailored and documented any potential business-required deviations from the configuration standards. In addition, OPM does not consistently run automated scans to verify that information systems are in compliance with pre-established configuration settings, as they have yet to be developed for all operating platforms. 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.

NIST SP 800-53, Revision 4, states 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 these systems being insecurely configured.

Recommendation 20 (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 develop, document and implement standard security configurations for all hardware devices and/or operating systems."

Recommendation 21 (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 20 has been completed.

OPM Response:

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

Recommendation 22 (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. With the implementation of the DHS CDM equipment and updated continuous monitoring processes, OPM plans to have all deviations identified and documented for regular review."

Metric 19 – Flaw Remediation and Patch Management

FY 2017 Maturity Level: 2 – Defined. OPM performs automated vulnerability and patch compliance scans on its systems on a routine basis. OPM's vulnerability scanning program has improved over the last year, but 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 own 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 vulnerability scan results to the various system owners so that they can remediate the weaknesses identified in the scans. Formal POA&M entries are created for weaknesses that require significant time to remediate. However, OPM does not have a process to record or track the remediation status for other routine security weaknesses identified during vulnerability scans.

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

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

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

Recommendation 23 (Rolled forward from FY 2014)

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

OPM Response:

"We concur with this recommendation. CSP plans to update its processes and procedures so that any vulnerability scans that are delayed or incomplete are effectively reinitiated to better track completion."

Recommendation 24 (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 concur with the recommendation. OPM plans to take a multifaceted approach to identify and remediate unsupported software and operating platforms that are being used within its network environment. OPM has made significant progress over the past year to replace unsupported operating platforms on its environment and will continue this effort in FY 2018."

Recommendation 25 (Rolled forward from FY 2014)

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

OPM Response:

"We concur with the recommendation. OCIO plans to integrate scanning tools with its system inventory so we can create POA&Ms directly from scan results."

Recommendation 26 (Rolled forward from FY 2014)

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

OPM Response:

"We partially concur with the recommendation. OPM has a patch management process in place for timely deployment of operating system patches. OPM plans to conduct an assessment and draft a plan to address timely deployment of third party vendor patches."

OIG Comment:

OPM states that it has a patch management process in place, but our independent test work detected instances where this process was not effective. The recommendation and the narrative supporting it are still applicable, and the recommendation remains open.

Metric 20 – Trusted Internet Connection Program

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

FY 2017 Maturity Level: 3 – Consistently Implemented. OPM has defined and implemented controls to monitor and manage its approved trusted internet connections (TIC). This has allowed

OPM to meet OMB requirements related to the TIC initiative. Any improvements that need to be made to the agency's current TIC controls are documented within the organization's POA&M.

Metric 21 – Configuration Change Control Management

FY 2017 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 a change to an information system. Our test work indicated that OPM 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 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, the agency has successfully implemented many Identity, Credential, and Access Management (ICAM) related security controls. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Identity, Credential, and Access Management domain is "3 – Consistently Implemented."**

Metric 23 – ICAM Roles, Responsibilities, and Resources

FY 2017 Maturity Level: 2 – Defined. OPM maintains policies and procedures that outline roles and responsibilities related to its agency-wide system account and identity management program. This includes procedures for creating user accounts with the appropriate level of access and procedures for removing access for terminated employees. However, OPM does not have a process in place to ensure that adequate resources (people, processes, and technology) are provided to stakeholders to fully implement ICAM controls.

FICAM Roadmap Implementation Guidance states that "As part of the [Logical Access Control Systems (LACS)] 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 LACS 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.

Recommendation 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.

OPM Response:

"We concur with this recommendation. OCIO is conducting an analysis of the current limitations of the ICAM program as a part of Phase 2 of the DHS Continuous Diagnostics and Mitigation (CDM) program. The goal is to identify the gaps to effectively implement an enterprise solution for provisioning and maintaining credentials for agency systems."

Metric 24 – ICAM Strategy

FY 2017 Maturity Level: 1 – Ad Hoc. 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 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.

OPM Response:

"We concur with this recommendation. OPM has conducted the "as-is" assessment and analysis and gaps have been identified. OPM is developing milestones to meet OPM and Federal security requirements. OPM plans to consider the adequacy of resources, processes and technology in the strategy for ICAM."

Metric 25 – Implementation of an ICAM Program

FY 2017 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) 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 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.

OPM Response:

"We concur with this recommendation. OCIO is conducting an analysis of the current limitations of the ICAM program as a part of Phase 2 of the DHS Continuous Diagnostics and Mitigation (CDM) program. The goal is to identify the gaps to effectively implement an enterprise solution for provisioning and maintaining credentials for agency systems. The outcome of this effort will include monitoring metrics to promote the overall completeness of the ICAM program."

Metric 26 – Personnel Risk

FY 2017 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 2017 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 2017 Maturity Level: 3 – Consistently Implemented. OMB Memorandum M-11-11 required all Federal information systems to use 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 not enforced PIV authentication to the vast majority of its applications.

OPM has enforced multi-factor authentication for non-privileged users for facility, network, and remote access through the use of PIV cards. The FY 2017 FISMA metrics state that these controls represent a "consistently implemented" strong authentication mechanism. However, 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. PIV authentication at the application level is only in place for 3 of OPM's 46 major applications.

Recommendation 30 (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 generally concur with the recommendation, to the extent it applies to systems where multi-factor authentication, including the use of PIV credentials, is feasible and appropriate. OPM plans to PIV-enable some applications in FY 2018; however, additional modernization efforts are necessary to PIV-enable other applications."

OIG Comment:

We agree that there are specific circumstances where PIV authentication is not appropriate (e.g., a system open to non-Government users that do not have a PIV card). However, the "feasibility" of upgrading legacy systems to use PIV authentication is not a legitimate reason to disagree with this recommendation. This is an OMB requirement as well as a critical control and should be a priority of the agency.

Metric 29 – Strong Authentication Mechanisms for Privileged Users

FY 2017 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 2017 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 2017 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.

FISCAM 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 31 (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. OPM plans to review and update its account management processes to secure network accounts after contractor termination actions are taken, in a timely manner, and in accordance with OPM security policies."

G. SECURITY TRAINING

FISMA requires all Government employees and contractors to take IT security awareness training on an annual basis. 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 33 – Security Training Policies and Procedures

FY 2017 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.

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

Metric 34 – Assessment of Workforce

FY 2017 Maturity Level: 1 – Ad Hoc. OPM has not defined a process for conducting an assessment of the knowledge, skills, and abilities of its workforce to determine employees' specialized training needs. The OCIO is working with the agency's human resources office to establish job codes that better identify the responsibilities and required skills for specific IT positions. This assessment will enable the OCIO to identify the gaps within the current workforce knowledge set and determine any future IT security 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 implement a process for identifying gaps within an IT security training program increases the risk that OPM staff is not fully prepared to address the security threats facing the agency.

Recommendation 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.

OPM Response:

"We concur with this finding. We are currently putting together the training plan and have procured additional training modules. This initiative is part of the current strategic plan for the Cybersecurity Program."

Metric 35 – Security Awareness Strategy

FY 2017 Maturity Level: 1 – Ad Hoc. OPM has not defined its security awareness and training strategy or created a plan to develop, implement, and maintain a security awareness program tailored to the mission and risk environment. After OPM completes its assessment to identify the IT security training needs of the agency, it should document a strategy to ensure that those training needs are met.

NIST SP 800-50, Section 3, requires an agency to ensure "[a] needs assessment is conducted and a training strategy is developed and approved. This strategic planning document identifies implementation tasks to be performed in support of established agency security training goals."

Failure to define a security awareness and training strategy decreases the effectiveness of the agency's overall security training program.

Recommendation 33

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

OPM Response:

"We concur with the recommendation. In FY 2017, OPM initiated an effort to document a security awareness and training strategy. This effort is being included in the security awareness and training program schedule[d] for FY 2018."

Metric 36 – Specialized Security Training Policies

FY 2017 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 37 – Tracking IT Security Training

FY 2017 Maturity Level: 3 – Consistently Implemented. 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. Over 96 percent of OPM's employees and contractors completed the security awareness training course in FY 2017.

Over 96 percent of OPM employees and contractors completed security awareness training.

Metric 38 – Tracking Specialized IT Security Training

FY 2017 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 has developed a table outlining the security training requirements (in terms of number of hours of training required) for specific job roles within OPM. The OCIO uses a spreadsheet to track the security training taken by employees that have been identified as having security responsibility. At least 95 percent of those employees with significant security responsibilities completed specialized IT security training in FY 2017.

Metric 39 – Security Training Other Information

There are no additional comments regarding the security training program.

H. 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 40 – ISCM Strategy

FY 2017 Maturity Level: 2 – Defined. OPM has developed an ISCM strategy that addresses the monitoring of security controls at the organization, business unit, and individual information system level. At the organization and business unit level, the ISCM strategy defines how the agency's activities support risk management in accordance with organizational risk tolerance. At the information system level, the ISCM strategy establishes processes for monitoring security controls for effectiveness and reporting any findings.

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

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

In FY 2017 only 9 of OPM's 46 systems were subject to adequate security controls testing and monitoring. It has been over 11 years since all OPM systems were subject to adequate security controls testing within a single fiscal year.

Only 9 of OPM's 46 systems were subject to adequate security controls testing and monitoring.

At this stage in the development of OPM's ISCM program the organization has not met its goal of providing stakeholders with sufficient information to evaluate risk. It is the responsibility of the ISSO for each major system to ensure that the security controls of each system are assessed

on a continuous basis. As discussed in section B, above, 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 indicative of a significant deficiency in the agency's information security governance structure.

Metric 41 – ISCM Policies and Procedures

FY 2017 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, as discussed in more detail under Metric 43, OPM has not adhered to its ISCM policies.

Metric 42 – ISCM Roles, Responsibilities, and Resources

FY 2017 Maturity Level: 2 – Defined. OPM has defined the structure, roles, and responsibilities of its ISCM teams and stakeholders. However, the weaknesses that we identified in OPM's ISCM program indicate that the agency does not have adequate resources to effectively implement the activities required by its ISCM strategy and policies. Furthermore, OPM has not implemented a process to identify the ISCM resource gaps it would need to fill in order 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 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.

OPM Response:

"We concur with this recommendation. The resource, budget, staffing, alignment challenges identified above impact CSP's ability to properly enforce compliance through ISSOs. Our work to address those issues, and restructure the office, will better enable CSP to address to this recommendation."

Metric 43 – Ongoing Security Assessments

FY 2017 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 multiple 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 that 9 of OPM's 46 major systems were subject to security controls testing in FY 2017 that complied with OPM's ISCM submission schedule.

It has been over 11 years since all OPM systems were subject to an adequate security controls test within a single fiscal year. FISMA requires agencies to "conduct assessments of security controls at a frequency appropriate to risk, but no less than annually."

Failure to complete a comprehensive security controls test for all information systems and using 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 35 (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. The resource, budget, staffing, alignment challenges identified above impact CSP's ability to properly enforce compliance through ISSOs. Our work to address those issues, and restructure the office, will better enable CSP to address to this recommendation."

Metric 44 – Measuring ISCM Program Effectiveness

FY 2017 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. In addition, OPM has defined the format and frequency of reports measuring its ISCM program effectiveness.

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

However, 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 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.

OPM Response:

"We concur with this recommendation. The resource, budget, staffing, alignment challenges identified above impact CSP's ability to properly enforce compliance through ISSOs. Our work to address those issues, and restructure the office, will better enable CSP to address to this recommendation."

Metric 45 – ISCM Other Information

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

I. 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 46 – Incident Response Policies, Procedures, Plans, Strategies

FY 2017 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 47 – Incident Roles and Responsibilities

FY 2017 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 48 – Incident Detection and Analysis

FY 2017 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.

Metric 49 – Incident Handling

FY 2017 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 50 – Sharing Incident Response Information

FY 2017 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 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.

Metric 51 – Contractual Relationships in Support of Incident Response

FY 2017 Maturity Level: 3 – Consistently Implemented. OPM collaborates with DHS and other parties, when needed, for technical assistance, surge resources, and any special requirements for quickly responding to incidents. OPM utilizes software tools provided by DHS for intrusion detection and prevention capabilities. OPM also uses third party contractors, when needed, to support incident response processes.

Metric 52 – Technology to Support Incident Response

FY 2017 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 53 – Incident Response Other Information

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

J. CONTINGENCY PLANNING

Contingency planning includes the policies and procedures that ensure adequate availability of information systems, data, and business processes. The sections below detail the results for each individual metric in this domain. **OPM's overall maturity level for the Contingency Planning domain is "2 – Defined."**

Metric 54 – Contingency Planning Roles and Responsibilities

FY 2017 Maturity Level: 3 – Consistently Implemented. 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.

Metric 55 – Contingency Planning Policies and Procedures

FY 2017 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 40 of OPM's 46 major information systems;
- The contingency plans for only 12 of OPM's 46 major systems were reviewed and updated in FY 2017;
- Only 5 of 46 contingency plans were tested in FY 2017; and
- Only 2 of 46 contingency plans were updated to address the test results.

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, above, we continue to believe that OPM's failure to meet long-standing FISMA metrics (such as the ones in this section related to

OPM's failure to test the contingency plans for almost 90 percent of its systems is a symptom of the significant deficiency in the agency's information security governance structure.

contingency planning) is indicative of a significant deficiency 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 long-standing issues at OPM.

Metric 56 – Business Impact Analysis

FY 2017 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 Business Impact Analysis (BIA) at the information system level. However, 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.

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 37

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

OPM Response:

"We concur with the recommendation. In FY 2018, OPM intends to begin planning for an agency-wide BIA, utilizing work done to support the agency's Continuity of Operations Plan."

Metric 57 – Contingency Plan Maintenance

FY 2017 Maturity Level: 2 – Defined. OPM has a policy in place that requires a contingency plan to be in place for every major information system, and that this plan be updated on a routine basis. However, OPM is not adhering to this policy. In FY 2017, we received evidence that contingency plans exist for only 40 of OPM's 46 major systems. Of those 40 contingency plans, only 12 had been reviewed and updated in FY 2017.

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 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 38 *(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. OPM intends to develop a plan to update contingency plans within the year and monitor progress to completion."

Metric 58 – Contingency Plan Testing

FY 2017 Maturity Level: 2 – Defined. Routinely testing contingency plans is a critical step in ensuring that plans can be successfully executed in the event of a disaster. Only 5 of the 46 major information systems were subject to an adequate contingency plan test in fiscal year 2017. Furthermore, contingency plans for 11 of 46 major systems have not been tested for 2 years or longer.

The Information Security Privacy and Policy Handbook requires system contingency plans be "tested and/or exercised at least annually using OPM defined and information system specific tests and exercises . . . ."

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 39 *(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. As the OPM contingency plans are updated, OCIO will assist system owners and project owners to test contingency plans annually."

Metric 59 – Information System Backup and Storage

FY 2017 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 60 – Communication of Recovery Activities

FY 2017 Maturity Level: 2 – Defined. OPM has polices in place that define how contingency plan activities are performed throughout the agency. As discussed above in Metric 57, 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 38 above addresses the deficiencies in this metric.

Metric 61 – Contingency Planning Other Information

There are no additional OIG 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	2	Risk Management and Contractor Systems Level 2: Defined	Identify Level 2: Defined	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 – Contracting 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	Identity and Access Management Level 3: Consistenty 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 – Security Training Policies and Procedures	3	Security Training Level 3: Consistently Implemented		
34 – Assessment of Workforce	1			
35 – Security Awareness Strategy	1			
36 – Specialized Security Training Policies	3			
37 – Tracking IT Security Training	3			
38 – Tracking Specialized IT Security Training	3			
39 – Security Training Other Information	n/a			
40 – ISCM Strategy	2	Continous Monitoring Level 2: Defined	Detect Level 2: Defined	
41 – ISCM Policies and Procedures	2			
42 – ISCM Roles, Responsibilities, and Resources	2			
43 – Ongoing Security Assessments	2			
44 – Measuring ISCM Program Effectiveness	2			
45 – ISCM Other Information	n/a			
46 – Incident Response Policies, Procedures, Plans, Strategies	4	Incident Response Level 4: Managed and Measurable	Respond Level 4: Managed and Measurable	
47 – Incident Roles and Responsibilities	4			
48 – Incident Detection and Analysis	3			
49 – Incident Handling	4			
50 – Sharing Incident Response Information	4			
51 – Contractual Relationships in Support of Incident Response	3			
52 – Technology to Support Incident Response	4			
53 – Incident Response Other Information	n/a			
54 – Contingency Planning Roles and Responsibilities	3	Contingency Planning Level 2: Defined	Recover Level 2: Defined	
55 – Contingency Planning Policies and Procedures	2			
56 – Business Impact Analysis	1			
57 – Contingency Plan Maintenance	2			
58 – Contingency Plan Testing	2			
59 – Information System Backup and Storage	3			
60 - Communication of Recovery Activities	2			
61 – Contingency Planning Other Information	n/a			

APPENDIX II – Status of Prior OIG Audit Recommendations

The table below outlines the current status of recommendations issued in the FY 2016 FISMA audit (Report No. 4A-CI-00-16-039, issued November 9, 2016).

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-00-17-020 Recommendation 1
2	We recommend that OPM thoroughly define the roles and responsibilities of all positions in its IT security management structure.	New recommendation for FY 2016	CLOSED: 6/6/2017
3	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-00-17-020 Recommendation 15
4	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-00-17-020 Recommendation 2
5	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-00-17-020 Recommendation 3
6	We recommend that the OPM Director consider shutting down information systems that do not have a current and valid Authorization.	Rolled forward in FY 2014	CLOSED: 6/6/2017
7	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-00-17-020 Recommendation 10

8	We recommend that OPM adhere to remediation dates for its POA&M weaknesses.	New recommendation for FY 2016	OPEN: Rolled forward as Report 4A-CI-00-17-020 Recommendation 11
9	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-00-17-020 Recommendation 4
10	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-00-17-020 Recommendation 5
11	We recommend that OPM improve its system inventory by correlating the elements of the inventory to the servers and information systems they reside on.	New recommendation for FY 2016	OPEN: Rolled forward as Report 4A-CI-00-17-020 Recommendation 6
12	We recommend that the OCIO develop and implement a baseline configuration for all operating platforms in use by OPM including, but not limited to, [redacted].	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-17-020 Recommendation 20
13	Where an OPM configuration standard is 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.	New recommendation in FY 2014	OPEN: Rolled forward as Report 4A-CI-00-17-020 Recommendation 22
14	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-00-17-020 Recommendation 23
15	We recommend that the OCIO implement a process to ensure that only supported software and operating platforms are used within the network environment.	New recommendation in FY 2016	OPEN: Rolled forward as Report 4A-CI-00-17-020 Recommendation 24
16	We recommend the OCIO conduct routine compliance scans against established baseline configurations for all servers and databases in use by OPM.	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-17-020 Recommendation 21
17	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-00-17-020 Recommendation 25
18	We recommend that the OCIO implement a process to apply operating system and third party vendor patches in a timely manner, which is defined within the OPM Information Security and Privacy Policy Handbook.	Rolled forward from FY 2014	OPEN: Rolled forward as Report 4A-CI-00-17-020 Recommendation 26

19	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.	New recommendation in FY 2016	OPEN: Rolled forward as Report 4A-CI-00-17-020 Recommendation 31
20	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-00-17-020 Recommendation 30
21	We recommend that the OCIO ensure that all employees with significant information security responsibility take meaningful and appropriate specialized security training on an annual basis.	New recommendation in FY 2016	CLOSED : 10/12/2017
22	We recommend that OPM continue to implement sufficient tools and controls to meet all requirements of CIGIE's Information Security Continuous Monitoring Maturity Model Level 3, "Consistently Implemented."	New recommendation in FY 2016	CLOSED with issuance of FY 2017 draft audit report: 9/25/2017
23	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-00-17-020 Recommendation 35
24	We recommend that OPM continue to implement sufficient tools and controls to meet all requirements of CIGIE's Incident Response Program Maturity Model Level 3, "Consistently Implemented."	Rolled forward from FY 2016	CLOSED with issuance of FY 2017 draft audit report: 9/25/2017
25	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-00-17-020 Recommendation 38
26	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 2008	OPEN: Rolled forward as Report 4A-CI-00-17-020 Recommendation 39

APPENDIX III

This appendix contains the U.S. Office of Personnel Management's October 11, 2017 response to the draft audit report, issued September 25, 2017.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

October 11, 2017

MEMORANDUM FOR [redacted]
CHIEF, INFORMATION SYSTEMS AUDIT GROUP
OFFICE OF THE INSPECTOR GENERAL

FROM: KATHLEEN M. MCGETTIGAN
ACTING DIRECTOR

Subject: Office of Personnel Management Response to the Office of the Inspector General Federal Information Security Modernization Act Audit – FY 2017 (Report No. 4A-CI-00-17-020)

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 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.

We welcome a collaborative dialogue to fully understand the OIG's recommendations as we plan our remediation efforts so that our actions and the closure of the recommendations thoroughly address the underlying issues. I look forward to continued discussions during our monthly reviews to remain aligned.

OPM appreciates OIG's recognition of our significant progress in several information security areas. OPM has taken steps to enhance its cybersecurity posture in multiple areas through: the addition of cybersecurity tools and security updates; staff and agency-wide training; hiring of critical personnel; and collaboration with OPM's interagency partners. OPM recognizes that cybersecurity is not just about technology, but is also about people. Therefore, in addition to strengthening technology, OPM has added seasoned cybersecurity and IT experts to an already talented team. OPM continues to leverage and utilize interagency partnerships and the expertise of the IT and cyber communities across government.

Although OPM values the OIG findings and recommendations in this audit, it is important to take stock of the fact that this is the first time OIG has utilized the maturity model in an audit of the OCIO. This report thus establishes a new baseline from which OPM and OIG will be working from Fiscal Year 2017 forward. We welcome a collaborative dialogue as we develop a mutual understanding of this maturity model and its underlying metrics.

We also note that the agency's ability to address a number of this audit's findings and recommendations will revolve around resource availability and capability. OCIO's resources impact the agency's ability to execute the mission, and one factor that diminishes capacity with existing resources has been audit fatigue. OIG is only one of several entities that audit all aspects of OCIO's programs, and each time an engagement commences, OCIO is obligated to expend time and resources locating responsive documents, responding to questions, and, ultimately, replying to these multiple, sometimes overlapping and duplicative, audits. We appreciate and understand the importance of these audits, but believe OCIO would benefit from an effort to achieve a more tailored, streamlined, and coordinated approach from its various auditors.

OCIO's resources have been impacted by budgetary uncertainties and the ensuing difficulties in planning hiring actions that can be sustained in upcoming fiscal years. Additionally, OPM Cybersecurity has had challenges restructuring its organization to better assign supervisors and team leads within the Cybersecurity Program (CSP) and anticipates that restructuring will enhance CSP's capabilities to address several of the recommendations OIG identifies, below, including enhancing CSP's ability to manage new policies, develop improved quality control mechanisms, and staff its priorities.

The impact of these resource and staffing issues is woven through many, if not all, of the OIG recommendations, below.

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. As discussed above, OCIO's resources have been impacted by budgetary uncertainties and the ensuing difficulties in planning and funding hiring actions in upcoming fiscal years. OPM faces challenges in its ability to prioritize cybersecurity positions over other agency hiring decisions. A gap also exists in OPM's ability to retain and backfill cybersecurity positions. The Agency priorities may not always align with the cybersecurity priorities. Additionally, OPM Cybersecurity has had challenges restructuring its organization to better assign supervisors and team leads within the Cybersecurity Program and anticipates that restructuring will enhance CSP's capabilities to address concerns the OIG raises, including enhancing CSP's ability to manage new policies and develop improved quality control mechanisms.

Recommendation 2
We recommend that all active systems in OPM's inventory have a complete and current Authorization.

Management Response: We partially concur with the recommendation. The OIG states in the report that 80% of OPM's information systems had a valid authorization by Q3, FY 2017; however, all OPM information systems held a valid authorization in early Q2, FY 2017. The OIG states in its report that there are documentation inconsistencies and incomplete or

inadequate independent testing of the system security controls that need to be addressed. In FY2017, OPM recognized areas where there are inconsistencies in documentation or further independent testing of security controls would be beneficial. After the Cybersecurity program is restructured and clarification on resources is provided, we anticipate additional improvements in the quality and consistency of the ATO packages through improved management and oversight.

Recommendation 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.

Management Response: We do not concur with the recommendation. The agency has taken, and will continue to take, OIG's recommendation under advisement. However, consultation with the subject matter experts within the Agency to determine whether and how to implement this recommendation is necessary and appropriate.

Recommendation 4
We recommend that the OCIO ensure that all ISAs are valid and properly maintained.

Management Response: We concur with the recommendation. An audit of VPN connections has been completed and an audit of firewall connections will be completed next in order to complete mapping of connections. OPM is putting new polices and quality assurance mechanisms in place so that all ISAs will be valid and properly maintained.

Recommendation 5
We recommend that the OCIO ensure that a valid MOU/A exists for every interconnection.

Management Response: We concur with the recommendation. OPM is putting new polices and quality assurance mechanisms in place to improve visibility and review of all interconnection MOU/As exist for each interconnection.

Recommendation 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.

Management Response: We concur with the recommendation. OPM and DHS Continuous Diagnostics and Mitigation (CDM) have implemented a solution for correlating these elements to FISMA system boundaries. Implementation progress has been limited due to the lack of system documentation available to identify servers and tie them to their systems. Efforts are underway to complete server system tagging to facilitate this effort.

Recommendation 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.

Management Response: We concur with the recommendation. OPM and DHS CDM have implemented a solution for correlating these elements to FISMA system boundaries. Implementation progress has been limited due to the lack of system documentation available to identify software. Efforts are underway to complete a white/black list of enterprise software to facilitate this effort.

Recommendation 8
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. Through its Risk Management Council, OPM plans to develop the agency's Enterprise Risk Management Framework and Policy during FY 2018. This will define the agency's risk management strategy.

Recommendation 9
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. OPM plans to make appropriate updates to its Enterprise Architecture to include relevant information security architecture elements.

Recommendation 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).

Management Response: We concur with the recommendation. During FY 2018, as OPM matures it Enterprise Risk Management Program, we will take into account the requirements related to the Risk Executive Function outlined in NIST SP 800-39.

Recommendation 11
We recommend that OPM adhere to remediation dates for its POA&M weaknesses.

Management Response: We concur with the recommendation. In FY2017, OPM introduced a new management process for reviewing POA&M content, including milestones and remediation dates for POA&Ms. OPM will continue to improve the process to support better milestone definition, identification of remediation dates, and POA&M reviews and updates.

Recommendation 12
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. In FY2017, OPM introduced a new management process for reviewing POA&M content, including milestones and remediation dates for POA&Ms. OPM will continue to improve the process to support better milestone

definition, identification of remediation dates, and POA&M reviews and updates.

Recommendation 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.

Management Response: We concur with this recommendation. The resource, budget, staffing, alignment challenges identified above impact CSP's ability to properly enforce compliance through ISSOs. Our work to address those issues, and restructure the office will better enable CSP to address to this recommendation.

Recommendation 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.

Management Response: We concur with the recommendation. OPM plans to explore options for an automated enterprise-wide risk management solution during FY 2018. However, acquisition of an automated tool will be subject to the availability of resources.

Recommendation 15
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 plans to update the SDLC by elevating best practices and lessons learned from IT PMOs engaged in Agile development. The new SDLC will also leverage recommendations from engagement with 18F to ensure OCIO benefits from recognized industry standards and processes along with practical first-hand experience. OPM will develop a plan and timeline to implement and enforce the updated SDLC policy.

Recommendation 16
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. OPM plans to conduct an analysis to better determine CM resource requirements.

Recommendation 17
We recommend that OPM develop a process to communicate any risks identified from its configuration management activities with the stakeholders of the agency's risk management and continuous monitoring programs. The agency should also document the lessons learned from its configuration management activities and update its configuration management plan as appropriate.

Management Response: We partially concur with this recommendation. OPM concurs with the recommendation to document lessons learned and update its configuration management plan. However, OPM has implemented processes and procedures to document and communicate risks identified through configuration management activities to Authorizing Officials. This process is defined in artifacts provided during the audit. OPM will work with the OIG to provide clarification, where needed.

Recommendation 18
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. OCIO plans to work with system owners across OPM to establish baseline configuration that will be kept under configuration control.

Recommendation 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.

Management Response: We concur with this recommendation. Currently OCIO performs compliance scans based on security configuration standards in compliance with OPM policy. Scans will be updated to align with approved architecture baselines and reports will be submitted to Authorizing Officials as part of the continuous monitoring process.

Recommendation 20
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 develop, document and implement standard security configurations for all hardware devices and/or operating systems.

Recommendation 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.

Management Response: We concur with the recommendation. OPM plans to develop, document and implement standard security configurations for all servers and databases.

Recommendation 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.

Management Response: We concur with the recommendation. With the implementation of the

DHS CDM equipment and updated continuous monitoring processes, OPM plans to have all deviations identified and documented for regular review.

Recommendation 23
We recommend that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.

Management Response: We concur with this recommendation. CSP plans to update its processes and procedures so that any vulnerability scans that are delayed or incomplete are effectively reinitiated to better track completion.

Recommendation 24
We recommend that the OCIO implement a process to ensure that only supported software and operating platforms are used within the network environment.

Management Response: We concur with the recommendation. OPM plans to take a multifaceted approach to identify and remediate unsupported software and operating platforms that are being used within its network environment. OPM has made significant progress over the past year to replace unsupported operating platforms on its environment and will continue this effort in FY 2018.

Recommendation 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.

Management Response: We concur with the recommendation. OCIO plans to integrate scanning tools with its system inventory so we can create POA&Ms directly from scan results.

Recommendation 26
We recommend 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. OPM has a patch management process in place for timely deployment of operating system patches. OPM plans to conduct an assessment and draft a plan to address timely deployment of third party vendor patches.

Recommendation 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.

Management Response: We concur with this recommendation. OCIO is conducting an analysis of the current limitations of the ICAM program as a part of Phase 2 of the DHS Continuous Diagnostics and Mitigation (CDM) program. The goal is to identify the gaps to effectively implement an enterprise solution for provisioning and maintaining credentials for agency systems.

Recommendation 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.

Management Response: We concur with this recommendation. OPM has conducted the "as-is" assessment and analysis and gaps have been identified. OPM is developing milestones to meet OPM and Federal security requirements. OPM plans to consider the adequacy of resources, processes and technology in the strategy for ICAM.

Recommendation 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.

Management Response: We concur with this recommendation. OCIO is conducting an analysis of the current limitations of the ICAM program as a part of Phase 2 of the DHS Continuous Diagnostics and Mitigation (CDM) program. The goal is to identify the gaps to effectively implement an enterprise solution for provisioning and maintaining credentials for agency systems. The outcome of this effort will include monitoring metrics to promote the overall completeness of the ICAM program.

Recommendation 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.

Management Response: We generally concur with the recommendation, to the extent it applies to systems where multi-factor authentication, including the use of PIV credentials, is feasible and appropriate. OPM plans to PIV-enable some applications in FY 2018; however, additional modernization efforts are necessary to PIV-enable other applications.

Recommendation 31
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. OPM plans to review and update its account management processes to secure network accounts after contractor termination actions are taken, in a timely manner, and in accordance with OPM security policies.

Recommendation 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.

Management Response: We concur with this finding. We are currently putting together the training plan and have procured additional training modules. This initiative is part of the current strategic plan for the Cybersecurity Program.

Recommendation 33
We recommend that OPM develop and document a security awareness and training strategy tailored to its mission and risk environment.

Management Response: We concur with the recommendation. In FY2017, OPM initiated an effort to document a security awareness and training strategy. This effort is being included in the security awareness and training program schedule for FY 2018.

[redacted]

Recommendation 35
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 concur with this recommendation. The resource, budget, staffing, alignment challenges identified above impact CSP's ability to properly enforce compliance through ISSOs. Our work to address those issues, and restructure the office, will better enable CSP to address to this recommendation.

Recommendation 36
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. The resource, budget, staffing, alignment challenges identified above impact CSP's ability to properly enforce compliance through ISSOs. Our work to address those issues, and restructure the office, will better enable CSP to address to this recommendation.

Recommendation 37
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 36

Management Response: We concur with this recommendation. The resource, budget, staffing, alignment challenges identified above impact CSP's ability to properly enforce compliance through ISSOs. Our work to address those issues, and restructure the office, will better enable

CSP to address to this recommendation.

Recommendation 38
We recommend that the OCIO conduct an agency-wide BIA and incorporate the results into the system-level contingency plans.

Management Response: We concur with the recommendation. In FY 2018, OPM intends to begin planning for an agency-wide BIA, utilizing work done to support the agency's Continuity of Operations Plan.

Recommendation 39
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. OPM intends to develop a plan to update contingency plans within the year and monitor progress to completion.

Recommendation 40
We recommend that OPM test the contingency plans for each system on an annual basis.

Management Response: We concur with the recommendation. As the OPM contingency plans are updated, OCIO will assist system owners and project owners to test contingency plans annually.

Again, thank you for the opportunity to provide comment. Please contact me or Mr. Dennis Coleman if you have questions or need additional information.

cc:
Jason D. Simmons
Chief of Staff

Dennis D. Coleman
Chief Financial Officer and Acting Chief Management Officer

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

Janet L. Barnes
Director, Internal Oversight and Compliance

David A. Garcia
Chief Information Officer

[redacted]
Chief Information Security Officer

Theodore M. Cooperstein
General Counsel

APPENDIX IV – Cyberscope Submission

This appendix contains the U.S. Office of Personnel Management Inspector General Federal Information Security Modernization Act of 2014 Cyberscope Reporting Metrics.

Inspector General

Section Report

2017

Annual FISMA Report

Office of Personnel Management

Function 1: Identify - Risk Management

1 Does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800-53: CA-3 and PM-5; OMB M-04-25; NIST Cybersecurity Framework (CSF): ID.AM-1 – 4)?

Defined (Level 2)

Comments: The U.S. Office of Personnel Management (OPM) has defined the policies and procedures for managing its inventory of systems and its interconnections. OPM maintains a repository for documenting its system inventories and system interconnections. The inventory includes all major information systems, but not all of the system interconnections.

2 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7 and CM-8; NIST SP 800-137; Federal Enterprise Architecture (FEA) Framework, v2)?

Defined (Level 2)

Comments: 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.

3 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53: CA-7, CM-8, and CM-10; NIST SP 800-137; FEA Framework, v2)?

Ad Hoc (Level 1)

Comments: OPM uses a software tool to maintain its centralized software inventory. The inventory has some standard data elements (e.g. name, owner, and description) but does not contain the level of detail necessary for thorough tracking and reporting (e.g., vendor, version, installation locations, license information, and information system association).

4 To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions (NIST SP 800-53: RA-2, PM-7, and PM-11; NIST SP 800-60; CSF: ID.BE-3; and FIPS 199)?

Consistently Implemented (Level 3)

Comments: OPM has implemented policies and procedures for categorizing its information and information systems that follow FIPS 199 and NIST SP 800-60 guidance.

Function 1: Identify - Risk Management

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy that include the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST 800-39; NIST 800-53: PM-8, PM-9; CSF: ID RM-1 – ID.RM-3; OMB A-123; CFO Council ERM Playbook)?

Ad Hoc (Level 1)

Comments: OPM has defined policies for risk management and recently created a Risk Management Council. The council serves as the risk executive function at OPM and develops the agency-wide risk management approach and guidance. The council has begun to meet regularly and has defined a risk profile for OPM, but has not yet established an overall risk strategy for the agency.

6 Has the organization defined an information security architecture and described how that architecture is integrated into and supports the organization's enterprise architecture to provide a disciplined and structured methodology for managing risk (NIST 800-39; FEA; NIST 800-53: PL-8, SA-3, and SA-8)?

Ad Hoc (Level 1)

Comments: OPM's enterprise architecture has not been updated since 2008, and it does not support the necessary integration of an information security architecture. OPM's IT environment has undergone significant changes since 2008, and while the agency has started to develop an information security architecture, it cannot complete the information security architecture without updating its enterprise architecture.

7 To what degree have roles and responsibilities of stakeholders involved in risk management, including the risk executive function/Chief Risk Officer, Chief Information Officer, Chief Information Security Officer, and other internal and external stakeholders and mission specific resources been defined and communicated across the organization (NIST 800-39: Section 2.3.1 and 2.3.2; NIST 800-53: RA-1; CSF: ID.RM-1 – ID.GV-2, OMB A-123, CFO Council ERM Playbook)?

Defined (Level 2)

Comments: OPM has defined the necessary roles and responsibilities of stakeholders in its risk management program. However, its Risk Management Council is not yet fulfilling all of the responsibilities of the risk executive function required by NIST.

8 To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53: CA-5; OMB M-04-25)?

Defined (Level 2)

Comments: This year OPM has made efforts to improve its POA&M process. In March, the Office of the Chief Information Officer (OCIO) released an updated POA&M policy that details the POA&M process and the roles and responsibilities of those involved. In addition, OPM has started using a new tracking tool for its POA&M repository. However, the lack of adequate security resources continues to impact OPM's ability to effectively manage its POA&Ms. Over 96 percent of POA&Ms were more than 30 days overdue, and over 88 percent were more than 120 days overdue.

Function 1: Identify - Risk Management

9 To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing
(i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework
(ii) internal and external asset vulnerabilities, including through vulnerability scanning,
(iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and
(iv) selecting and implementing security controls to mitigate system-level risks (NIST 800--37; NIST 800-39; NIST 800--53: PL-2, RA-1; NIST 800-30; CSF:ID.RA-1 – 6)?

Defined (Level 2)

Comments: OPM has defined the policies and procedures for conducting risk assessments for individual information systems. We reviewed a sample of risk assessments for systems that were authorized in FY 2017, and noted that a majority had issues 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.

10 To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123)?

Consistently Implemented (Level 3)

Comments: OPM has implemented policies and procedures to communicate information about risks across the agency.

11 To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (FAR Case 2007--004; Common Security Configurations; FAR Sections: 24.104, 39.101, 39.105, 39.106, 52.239-1; President's Management Council; NIST 800-53: SA-4; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; FY 2017 CIO FISMA Metrics: 1.7, 1.8)?

Consistently Implemented (Level 3)

Comments: OPM policy mandates the use of specific contracting language and service level agreements to ensure contractors meet both Federal and OPM standards.

Function 1: Identify - Risk Management

12 To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?

Ad Hoc (Level 1)

Comments: OPM does not have a centralized system or tool to view enterprise-wide risk information, nor has it defined requirements to develop one. 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 agency-wide risk information in a centralized location.

13.1 Please provide the assessed maturity level for the agency's Identify - Risk Management function.

Defined (Level 2)

Comments: Defined (Level 2)

13.2 Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

System Development Life Cycle

Comments: As noted in the FY 2016 OIG FISMA audit report, OPM has a long history of troubled system development projects. At the end of FY 2013, the OCIO published a new Systems Development Lifecycle (SDLC) policy, which was a significant first step in implementing a centralized SDLC methodology at OPM. The new SDLC policy incorporated several prior OIG recommendations related to a centralized review process of system development projects. However, this SDLC has not been actively enforced for all IT projects in the Agency. In FY 2016, the Agency's enormous IT infrastructure overhaul initiative was scrapped and divided into multiple parallel efforts to consolidate and modernize OPM's IT infrastructure. While our concerns with the Agency's infrastructure improvement project are reported separately from our FISMA audits, we have ongoing concerns that OPM's failure to follow a comprehensive SDLC will result in information systems not being properly managed throughout the lifecycle and that new projects will fail to meet the stated objectives, timelines, and budgets.

Calculated Maturity Level - Defined (Level 2)

Function 2A: Protect - Configuration Management

Function 2A: Protect - Configuration Management

14 To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800- 53: CM-1; SP 800-128: Section 2.4)?

Defined (Level 2)

Comments: OPM has policies and procedures in place defining configuration management (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.

15 To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate location within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contracted systems (NIST 800--128: Section 2.3.2; NIST 800--53: CM-9)?

Defined (Level 2)

Comments: 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. 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.

16 To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53: CM-1; NIST 800-128: 2.2.1)

Defined (Level 2)

Comments: OPM has defined organization-wide CM policies and procedures, but has not consistently implemented many of the controls outlined these policies, such as:
- Establish and maintain baseline configurations and inventories of information systems;
- Routinely verify that information systems are actually configured in accordance with baseline configurations; and
- Conduct routine vulnerability scans on all information systems and remediate any vulnerabilities identified from the scan results in a timely manner.

17 To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53: CM-2, CM-8; FY 2017 CIO FISMA Metrics: 1.4, 1.5, and 2.1; CSF: ID.DE.CM-7)?

Ad Hoc (Level 1)

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

Function 2A: Protect - Configuration Management

18 To what extent does the organization utilize configuration settings/common secure configurations for its information systems (NIST SP 800-53: CM-6, CM-7, and SI-2; FY 2017 CIO FISMA Metrics: 2.2; SANS/CIS Top 20 Security Controls 3.7)?

Ad Hoc (Level 1)

Comments: OPM currently leverages several common best-practice configuration setting standards for its information systems. However, OPM has not documented a standard security configuration setting for all of its operating platforms and has not tailored and documented any potential business required deviations from the configuration standards.

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53: CM-3, SI-2; NIST 800-40, Rev. 3; OMB M-16-04; SANS/CIS Top 20 Control 4.5; and DHS Binding Operational Directive 15-01)?

Defined (Level 2)

Comments: OPM performs automated vulnerability and patch compliance scans on its systems on a routine basis. OPM's vulnerability scanning program has improved over the last year, but 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 own independent vulnerability scans indicate that OPM's production environment contains many instances of unsupported software and operating platforms.

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (FY 2017 CIO Metrics: 2.26, 2.27, 2.29; OMB M-08-05)?

Consistently Implemented (Level 3)

Comments: OPM has defined and implemented controls to monitor and manage its approved trusted internet connections.

21 To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST 800-53: CM--2, CM-3)?

Consistently Implemented (Level 3)

Comments: OPM has developed and documented policies and procedures for controlling configuration changes. Our test work indicated that OPM is consistently adhering to its change control procedures.

Function 2A: Protect - Configuration Management

22 Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?

n/a

Calculated Maturity Level - Defined (Level 2)

Function 2B: Protect - Identity and Access Management

23 To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST 800-53: AC-1, IA-1, PS-1; and the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

Defined (Level 2)

Comments: OPM maintains policies and procedures that outline roles and responsibilities related to its agency-wide system account and identity management program. However, OPM does not have a process in place to ensure that adequate resources (people, processes, and technology) are provided to stakeholders to fully implement ICAM controls.

24 To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?

Ad Hoc (Level 1)

Comments: 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.

25 To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 27 through 31) (NIST 800-53: AC-1 and IA--1; Cybersecurity Strategy and Implementation Plan (CSIP); and SANS/CIS Top 20: 14.1)?

Consistently Implemented (Level 3)

Comments: OPM has consistently implemented many of the required elements of a comprehensive ICAM program (see Metrics 26 - 31). However, OPM has not implemented PIV at the application level (see metric 28), and does not adequately manage contractor accounts (see metric 32).

Function 2B: Protect - Identity and Access Management

26 To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53: PS-2, PS- 3; and National Insider Threat Policy)?

Managed and Measurable (Level 4)

Comments: OPM has defined and implemented processes for assigning personnel risk designations and performing appropriate screenings prior to granting access to its systems.

27 To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non- privileged users) that access its systems are completed and maintained (NIST SP 800--53: AC-8, PL-4, and PS-6)?

Consistently Implemented (Level 3)

Comments: OPM has defined and implemented its processes for developing, documenting and maintaining access agreements for all users of the network.

28 To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800--53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

Consistently Implemented (Level 3)

Comments: OPM has enforced multi-factor authentication for non-privileged users for facility, network, and remote access through the use of PIV cards. However, PIV authentication at the application level is only in place for 3 of OPM's 46 major applications.

29 To what extent has the organization implemented strong authentication mechanisms (PIV or Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800--53: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; and Cybersecurity Sprint)?

Consistently Implemented (Level 3)

Comments: OPM has enforced multi-factor authentication for privileged user access to the OPM network and its backend servers.

30 To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2017 CIO FISMA metrics: Section 2; NIST SP 800-53: AC-1, AC-2 (2), AC-17; CSIP)?

Consistently Implemented (Level 3)

Comments: OPM has developed and implemented processes for provisioning, managing, and reviewing privileged user accounts.

Function 2B: Protect - Identity and Access Management

31 To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53: AC--17, SI-4; and FY 2017 CIO FISMA Metrics: Section 2)?

Managed and Measurable (Level 4)

Comments: 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.

32 Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?

Contractor Management

Comments: 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 the contractors that 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.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2C: Protect - Security Training

33 To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST 800-53: AT-1; and NIST SP 800-50)?

Consistently Implemented (Level 3)

Comments: OPM has developed and established an agency-wide IT security awareness training program.

Function 2C: Protect - Security Training

34 To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST 800-53: AT-2 and AT-3; NIST 800-50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181 (Draft); and CIS/SANS Top 20: 17.1)?

Ad Hoc (Level 1)

Comments: OPM has not defined a process for conducting an assessment of the knowledge, skills, and abilities of its workforce to determine employees' specialized training needs.

35 To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST 800--53: AT-1; NIST 800-50: Section 3))

Ad Hoc (Level 1)

Comments: OPM has not defined its security awareness and training strategy or created a plan to develop, implement, and maintain a security awareness program tailored to the mission and risk environment.

36 To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity questions 37 and 38 below) (NIST 800-53: AT-1 through AT-4; and NIST 800-50)

Consistently Implemented (Level 3)

Comments: OPM has established policies and procedures that require agency employees to take security awareness and specialized security training.

37 To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: Awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST 800-53: AT-2; FY 17 CIO FISMA Metrics: 2.23; NIST 800-50: 6.2; SANS Top 20: 17.4)

Consistently Implemented (Level 3)

Comments: The OCIO provides annual IT security and privacy awareness training to all OPM users through an interactive web-based course.

Function 2C: Protect - Security Training

38 To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST 800-53: AT-3 and AT-4; FY 17 CIO FISMA Metrics: 2.23)?

Consistently Implemented (Level 3)

Comments: OPM employees with significant information security responsibilities are required to take specialized security training in addition to the annual awareness training.

39.1 Please provide the assessed maturity level for the agency's Protect - Configuration Management/Identity and Access Management/Security Training (Functions 2A - 2C).

Consistently Implemented (Level 3)

Comments: Consistently Implemented (Level 3)

39.2 Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?

n/a

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 3: Detect - ISCM

40 To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organization-wide approach to ISCM (NIST SP 800-137: Sections 3.1 and 3.6)?

Defined (Level 2)

Comments: OPM has developed an ISCM strategy that addresses the monitoring of security controls at the organization, business unit, and individual information system level. However, in practice, OPM is not consistently implementing several of the objectives outlined in its ISCM strategy, including:
- "Security controls must be assessed to ensure continued effectiveness of their implementation and operation;"
- "Identified threats and vulnerabilities must be reported timely to support risk management decisions;" and
- "Feedback must be collected frequently and incorporated into a system of continually improving processes."

Function 3: Detect - ISCM

41 To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53: CA-7). (Note: The overall maturity level should take into consideration the maturity of question 43)

Defined (Level 2)

Comments: OPM has developed ISCM policies and procedures that have been tailored to OPM's environment and include specific requirements and deliverables. However, as discussed in more detail under Metric 43, OPM has not adhered to its ISCM policies.

42 To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53: CA-1; NIST SP 800-137; and FY 2017 CIO FISMA Metrics)?

Defined (Level 2)

Comments: OPM has defined the structure, roles, and responsibilities of its ISCM teams and stakeholders. However, the weaknesses that we identified in OPM's ISCM program indicate that the agency does not have adequate resources to effectively implement the activities required by its ISCM strategy and policies. Furthermore, OPM has not implemented a process to identify the ISCM resource gaps it would need to fill in order to effectively implement its ISCM program.

43 How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800-137: Section 2.2; NIST SP 800-53: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; OMB M-14-03)?

Defined (Level 2)

Comments: 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.

44 How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?

Defined (Level 2)

Comments: 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. In addition, OPM has defined the format and frequency of reports measuring its ISCM program effectiveness. However, 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.

Function 3: Detect - ISCM

45.1 Please provide the assessed maturity level for the agency's Detect - ISCM function.

Defined (Level 2)

Comments: Defined (Level 2)

45.2 Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?

n/a

Calculated Maturity Level - Defined (Level 2)

Function 4: Respond - Incident Response

46 To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53: IR-1; NIST 800-61 Rev. 2; FY 2017 CIO FISMA Metrics: 4.1, 4.3, and 4.6)? (Note: The overall maturity level should take into consideration the maturity of questions 48 - -52)

Managed and Measurable (Level 4)

Comments: OPM's incident response policies, procedures, plans, and strategies have been defined, communicated, and consistently implemented.

47 To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-16-03; OMB M-16-04; FY 2017 CIO FISMA Metrics: 1.6 and 4.5; and US-CERT Federal Incident Notification Guidelines)?

Managed and Measurable (Level 4)

Comments: 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.

48 How mature are the organization's processes for incident detection and analysis (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; US- CERT Incident Response Guidelines)?

Consistently Implemented (Level 3)

Comments: 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.

Function 4: Respond - Incident Response

49 How mature are the organization's processes for incident handling (NIST 800-53: IR-4)?

Managed and Measurable (Level 4)

Comments: OPM has defined its processes for incident handling in an incident response manual.

50 To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-16-03; NIST 800-53: IR-6; US-CERT Incident Notification Guidelines)?

Managed and Measurable (Level 4)

Comments: OPM has a documented policy that defines how incident response information will be shared with individuals with significant security responsibility.

51 To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents and enter into contracts, as appropriate, for incident response support (FY 2017 CIO FISMA Metrics: 4.4; NIST SP 800-86)?

Consistently Implemented (Level 3)

Comments: OPM collaborates with DHS and other parties, when needed, for technical assistance, surge resources, and any special requirements for quickly responding to incidents.

52 To what degree does the organization utilize the following technology to support its incident response program?

- Web application protections, such as web application firewalls
- Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools
- Aggregation and analysis, such as security information and event management (SIEM) products
- Malware detection, such as antivirus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2)

Managed and Measurable (Level 4)

Comments: 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.

53.1 Please provide the assessed maturity level for the agency's Respond - Incident Response function.

Managed and Measurable (Level 4)

Comments: Managed and Measurable (Level 4)

Function 4: Respond - Incident Response

53.2 Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?

n/a

Calculated Maturity Level - Managed and Measurable (Level 4)

Function 5: Recover - Contingency Planning

54 To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST 800-53: CP-1 and CP-2; NIST 800-34; NIST 800-84; FCD-1: Annex B)?

Consistently Implemented (Level 3)

Comments: OPM has a policy in place that describes the roles and responsibilities of individuals that are part of the agency's contingency planning program.

55 To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate? (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 56-60) (NIST SP 800-34; NIST SP 800--161).

Defined (Level 2)

Comments: 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 40 of OPM's 46 major information systems;
- The contingency plans for only 12 of OPM's 46 major systems were reviewed and updated in FY 2017;
- Only 5 of 46 contingency plans were tested in FY 2017; and
- Only 2 of 46 contingency plans were updated to address the test results.

56 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST 800-53: CP-2; NIST 800--34, Rev. 1, 3.2, FIPS 199, FCD--1, OMB M-17-09)?

Ad Hoc (Level 1)

Comments: OPM currently has a process in place to develop Business Impact Analysis (BIA) at the information system level. However, 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.

Function 5: Recover - Contingency Planning

57 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST 800-53: CP-2; NIST 800-34)?

Defined (Level 2)

Comments: OPM has a policy in place that requires a contingency plan to be in place for every major information system, and that this plan be updated on a routine basis. However, OPM is not adhering to this policy. In FY 2017 we received evidence that contingency plans exist for 40 of OPM's 46 major systems. Of those 40 contingency plans, only 12 had been reviewed and updated in FY 2017.

58 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST 800-34; NIST 800-53: CP-3, CP-4)?

Defined (Level 2)

Comments: Routinely testing contingency plans is a critical step in ensuring that plans can be successfully executed in the event of a disaster. Only 5 of the 46 major information systems were subject to an adequate contingency plan test in fiscal year 2017. Furthermore, contingency plans for 11 of 46 major systems have not been tested for 2 years or longer.

59 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST 800--53: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD1; NIST CSF: PR.IP- 4; and NARA guidance on information systems security records)?

Consistently Implemented (Level 3)

Comments: OPM has implemented processes, strategies, and technologies for information system backup and storage.

60 To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST 800-53: CP-2, IR-4)?

Defined (Level 2)

Comments: OPM has polices in place that define how contingency plan activities are performed throughout the agency. As discussed above in Metric 57, 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.

61.1 Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.

Defined (Level 2)

Comments: Defined (Level 2)

Function 5: Recover - Contingency Planning

61.2 Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?

n/a

Calculated Maturity Level - Defined (Level 2)

Function 0: Overall

0.1 Please provide an overallIG self-assessment rating (Effective/Not Effective)

Not Effective

Comments: OPM has a well-defined cybersecurity program, but it is not consistently or effectively implemented; see 0.2 for additional details.

Function 0: Overall

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

OPM overall maturity level: 2 - Defined.

Function 0: Overall

Comments:

In fiscal year (FY) 2017, the U.S. Office of Personnel Management (OPM)'s overall cybersecurity maturity level is measured as "2 - Defined." This assessment is based on the state of OPM's agency-wide information security program and activities throughout FY 2017.

Our audit determined that OPM has improved its Security Assessment and Authorization (Authorization) program. We upgraded the previous material weakness related to Authorizations to a significant deficiency for FY 2017 based on OPM's "Authorization Sprint" and the agency's continued efforts to maintain Authorizations for all information systems.

This audit report also rolls-forward a significant deficiency related to OPM's information security management structure. OPM is not making substantial progress in implementing our FISMA recommendations from prior audits. While resource limitations certainly impact the effectiveness of OPM's cybersecurity program, the staff currently in place is not fulfilling its responsibilities that are outlined in OPM policy and required by FISMA.

For the five cybersecurity framework functions, OPM received a maturity rating of "2 - Defined" for the functional areas of Identify, Detect, and Recover, received a rating of "3 - Consistently Implemented" for Protect, and a rating of "4 - Managed and Measurable" for Respond. The sections below provide a high level outline of OPM's performance in each of the seven cybersecurity framework domains:

Risk Management: "2 - Defined"
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: "2 - Defined"
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): "3 - Consistently Implemented"
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.

Function 0: Overall

Security Training: “3 - Consistently Implemented”
OPM has several opportunities for improvement within its IT security training program. OPM needs to ensure that all employees with significant security responsibilities take specialized IT security training.

Information Security Continuous Monitoring (ISCM): “2 - Defined”
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 recommendation has been open for over a decade.

Incident Response: “4 - Managed and Measurable”
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 level of “consistently implemented” or higher.

Contingency Planning: “2 - Defined”
OPM has not implemented several of the FISMA requirements related contingency planning, and continues to struggle with maintaining its contingency plans as well as conducting contingency plan tests on a routine basis.

APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

Function	Count
Ad-Hoc	4
Defined	5
Consistently Implemented	3
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	2
Defined	4
Consistently Implemented	2
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	1
Defined	1
Consistently Implemented	5
Managed and Measurable	2
Optimized	0
Function Rating: Consistently Implemented (Level 3)	0

Function 2C: Protect - Security Training

Function	Count
Ad-Hoc	2
Defined	0
Consistently Implemented	4
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3)	0

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	5
Consistently Implemented	0
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	2
Managed and Measurable	5
Optimized	0
Function Rating: Managed and Measurable (Level 4)	0

Function 5: Recover - Contingency Planning

Function	Count
Ad-Hoc	1
Defined	4
Consistently Implemented	2
Managed and Measurable	0
Optimized	0
Function Rating: Defined (Level 2)	0

Maturity Levels by Function

Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)
Function 2: Protect - Configuration Management / Identity Management / Security Training	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
Function 3: Detect - ISCM	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)
Function 4: Respond - Incident Response	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)
Function 5: Recover - Contingency Planning	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)
Overall	Not Effective	Not Effective	

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

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu