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 2016

Report Number 4A-CI-00-16-039
November 9, 2016

-- CAUTION --

EXECUTIVE SUMMARY

Federal Information Security Modernization Act Audit – FY 2016

Report No. 4A-CI-00-16-039 **November 9, 2016**

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). 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 instructions.

What Did We Audit?

The Office of the Inspector General has completed a performance audit of OPM's general FISMA compliance efforts in the specific areas defined in DHS's guidance and the corresponding reporting instructions. Our audit was conducted from April through September 2016 at OPM headquarters in Washington, D.C.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

This audit report again communicates a material weakness related to OPM's Security Assessment and Authorization (Authorization) program. In April 2015, the then Chief Information Officer 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. Although the moratorium on Authorizations has since been lifted, the effects of the April 2015 memorandum continue to have a significant negative impact on OPM. At the end of fiscal year (FY) 2016, the agency still had at least 18 major systems without a valid Authorization in place.

However, OPM did initiate an "Authorization Sprint" during FY 2016 in an effort to get all of the agency's systems compliant with the Authorization requirements. We acknowledge that OPM is once again taking system Authorization seriously. We intend to perform a comprehensive audit of OPM's Authorization process in early FY 2017.

This audit report also re-issues a significant deficiency related to OPM's information security management structure. Although OPM has developed a security management structure that we believe *can* be effective, there has been an extremely high turnover rate of critical positions. The negative impact of these staffing issues is apparent in the results of our current FISMA audit work. There has been a significant regression in OPM's compliance with FISMA requirements, as the agency failed to meet requirements that it had successfully met in prior years. We acknowledge that OPM has placed significant effort toward filling these positions, but simply having the staff does not guarantee that the team can effectively manage information security and keep OPM compliant with FISMA requirements. We will continue to closely monitor activity in this area throughout FY 2017.

The following page summarizes the results of this FY 2016 FISMA audit.

EXECUTIVE SUMMARY

Federal Information Security Modernization Act Audit – FY 2016

Summary of FY 2016 FISMA Results

- The material weakness related to OPM's Authorization program is reported again.
- A significant deficiency related to OPM's information security management structure has been re-opened (this was previously a material weakness that was closed).
- OPM has not adequately defined the roles and responsibilities for all positions within its IT management structure.
- OPM's system development life cycle policy is not enforced for all system development projects.
- OPM has made improvements to its continuous monitoring program and is now rated as Level 2 ("Defined") based upon the Council of the Inspectors General on Integrity and Efficiency (CIGIE) maturity model.
- OPM has also made improvements to its security incident program and is now rated as Level 2 ("Defined") based upon the CIGIE maturity model.
- OPM has developed an inventory of servers, databases, and network devices, but its overall inventory management program could be improved.
- OPM does not have configuration baselines for all operating platforms. This deficiency impacts the agency's ability to effectively audit and monitor systems for compliance.
- OPM has made progress in its vulnerability management program. However, improvements are needed in both the scanning and remediation processes.
- Multi-factor authentication is not required to access OPM systems in accordance with U.S. Office of Management and Budget memorandum M-11-11.
- OPM has not fully established a Risk Executive Function.
- Many individuals with significant information security responsibility have not taken specialized security training in accordance with OPM policy.
- The majority of OPM systems contain Plan of Action and Milestones that are over 120 days overdue.
- The contingency plans for most of OPM's systems have not been reviewed or tested in FY 2016.
- Several information security agreements and memoranda of understanding between OPM and contractor-operated information systems have expired.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
CIGIE	**Council of the Inspectors General on Integrity and Efficiency**
DHS	**U.S. Department of Homeland Security**
FACES	**Federal Annuity Claims Expert System**
FIPS	**Federal Information Processing Standards**
FISCAM	**Federal Information System Controls Audit Manual**
FISMA	**Federal Information Security Modernization Act**
FY	**Fiscal year**
IOC	**Internal Oversight and Compliance**
ISA	**Interconnection Security Agreements**
ISCM	**Information Systems Continuous Monitoring**
ISSO	**Information System Security Officer**
IT	**Information Technology**
ITPM	**IT Project Manager**
MOU/A	**Memorandum of Understanding/Agreement**
NIST	**National Institute for 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**
RMF	**Risk Management Framework**
SDLC	**System Development Life Cycle**
SP	**Special Publication**
VPN	**Virtual private network**

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) 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 IT resources owned and/or operated by a contractor supporting agency systems.

FISMA re-emphasizes the Chief Information Officer's strategic, agency-wide security responsibility. At OPM, security responsibility is assigned to the agency's Office of the Chief Information Officer (OCIO). FISMA also clearly places responsibility on each agency program office 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 Department of Homeland Security (DHS) Office of Cybersecurity and Communications issued the Fiscal Year (FY) 2016 Inspector General FISMA Reporting Instructions. This document provides a consistent form and format for agencies to report FISMA audit results to DHS. It identifies a series of reporting topics that relate to specific agency responsibilities outlined in FISMA. Our audit and reporting strategies were designed in accordance with the above 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 information technology (IT) security program in accordance with DHS's FISMA IG reporting requirements:

- Risk Management;
- Contractor Systems;
- Configuration Management;
- Identity and Access Management;
- Security and Privacy Training;
- Information Security Continuous Monitoring;
- Incident Response Program; and
- Contingency Planning.

In addition, we evaluated the status of OPM's IT security governance structure and the agency's system Authorization process, 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 1), and performed an audit focused on one of OPM's major information systems – the Federal Annuity Claims Expert System (FACES).

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 2016.

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 an information security audit on the FACES major information system. We considered the internal control structure for various OPM systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls for these various systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of these systems'

internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented. As appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

In conducting our audit, we relied to varying degrees on computer-generated data provided by OPM. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. However, we believe that the data was sufficient to achieve the audit objectives, and nothing came to our attention during our audit to cause us to doubt its reliability.

Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the set of internal controls for these various systems taken as a whole.

The criteria used in conducting this audit included:

- DHS Office of Cybersecurity and Communications FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics;
- OPM Information Technology Security and Privacy Policy Handbook;
- OPM Information Technology Security FISMA Procedures;
- OPM Security Assessment and Authorization Guide;
- OPM Plan of Action and Milestones Standard Operating Procedures;
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive 12;
- P.L. 107-347, Title III, Federal Information Security Management Act of 2002;
- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- National Institute for Standards and Technology (NIST) Special Publication (SP) 800-12, 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, Guide for Mapping Types of Information and Information Systems to Security Categories;
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems;
- FIPS Publication 140-2, Security Requirements for Cryptographic Modules; and
- Other criteria as appropriate.

The audit was performed by the OIG at OPM, as established by the Inspector General Act of 1978, as amended. Our audit was conducted from April through September 2016 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. Information Security Governance

Information security governance is the overall framework and supporting management structure and processes that are the foundation of a successful information security program. Proper governance requires agency management to proactively implement cost-effective controls to protect the critical information systems that support the core mission, while managing the changing risk environment. 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.

The following sections provide additional details of our review of IT security governance at OPM.

1) Security Management Structure

For many years, we reported increasing concerns about the state of OPM's information security governance. Our FISMA audit reports from FY 2009 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.

Our FY 2014 FISMA report reduced the severity of the material weakness to a significant deficiency based on OPM's *plan* to hire enough ISSOs to manage the security for all of OPM information systems. In FY 2015, OPM successfully filled the vacant ISSO positions, effectively centralizing IT security responsibility under the Chief Information Officer (CIO). With this new governance structure in place, we closed the audit recommendation related to security management structure and removed the significant deficiency from our report.

For a brief period of time, this governance structure was operating effectively. However, there has been an extremely high employee turnover rate for the ISSO positions, and OPM has struggled to backfill these vacancies. In addition, there have been five different individuals in the role of the Chief Information Officer in the past three years.

The negative impact of these staffing issues is apparent in the results of our current FISMA audit work. There has been a significant regression in OPM's compliance with FISMA requirements, as the agency failed to meet requirements that it had successfully met in prior years.

We believe that OPM's IT security management structure – as currently defined on paper – can be effective with some minor improvements (see the next section of this report). However, this structure was not operational for the majority of FY 2016, and therefore we believe that this issue again rises to the level of a significant deficiency.

OPM's security management structure is reported as a significant deficiency, but the agency made recent progress in filling critical IT security positions.

Although OPM's security management structure was not effective throughout FY 2016, there has been recent progress in hiring additional ISSOs. OPM currently has 16 ISSOs on its security team; enough to manage security for all of the agency's major information systems. The agency also hired a new permanent Chief Information Security Officer. However, simply having the staff on board does not guarantee that the team can effectively manage information security and keep OPM compliant with FISMA requirements. We will continue to closely monitor this team's activity throughout FY 2017.

Recommendation 1

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

OPM Response:

"We concur with the recommendation. In FY 2016, OPM hired eight ISSOs bringing the total to 16 ISSOs currently in place. The Office of the Chief Information Officer (OCIO) is hiring an additional eight ISSOs, three of which are now onboarding, for a total of 24 ISSO positions, which will support all of OPM's major information systems."

OIG Comment:

As part of the audit resolution process, we recommend that OPM provide its Internal Oversight and Compliance (IOC) division with evidence that it has fully implemented this recommendation. This statement applies to all subsequent recommendations that OPM agrees to implement.

2) Security Roles and Responsibilities

OPM must more thoroughly define the roles and responsibilities of all positions in its IT security management structure.

As noted above, OPM has designed (but not fully implemented) an information security management structure. One opportunity for improvement for this structure would be to more thoroughly define the roles and responsibilities of the individuals responsible for IT security and operations. Each ISSO position is complemented by an IT Project Manager (ITPM) position that typically has more operational (as opposed to security) responsibility. Throughout the fieldwork phase of this audit it became apparent to us that there is widespread confusion regarding whether certain responsibilities belong to the ISSO or the ITPM. One instance of this confusion came during our walkthrough of the vulnerability scanning process, where it was unclear to the individuals that received the scan results who would remediate and track the weaknesses identified. We understand that OPM is working on a draft document further defining the ISSO and ITPM roles and responsibilities, but it is still being developed and requires formal approval.

NIST SP 800-53, Revision 4, requires that an organization "Designates individuals to fulfill specific roles and responsibilities within the organization's risk management process."

The lack of clearly defined roles and responsibilities within the security management structure increases the risk that critical security processes are improperly managed or simply ignored.

Recommendation 2

We recommend that OPM thoroughly define the roles and responsibilities of all positions in its IT security management structure.

OPM Response:

"We concur with the recommendation. OCIO is finalizing the updated IT security policies and procedures involving the positions within the IT security management structure in the OCIO, including updated roles and responsibilities."

3) Systems Development Lifecycle Methodology

As noted in last year's FISMA report, OPM has a history of troubled system development projects. Despite multiple attempts and hundreds of millions of dollars invested, OPM

has encountered well publicized failures to modernize its retirement claims processing, financial, and background investigation systems. In FY 2016, the agency's enormous IT infrastructure overhaul initiative was significantly behind schedule. In our opinion, the root causes of these issues are related to the lack of centralized oversight of systems development.

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 new SDLC is only applicable to major investment projects, and thus is not actively enforced for all IT projects in the agency. OCIO's response to last year's recommendation stated that "A plan and timeline for implementation of the policy for all Development, Modernization and Enhancement (DM&E) projects is also being developed." As a part of this current audit we requested the current plan and timeline for implementing the SDLC framework. The response was that "there is no implementation timeline."

While our concerns with the agency's infrastructure improvement project are reported separately from our FISMA audits, we have ongoing concerns that OPM's lack of a comprehensive SDLC will result in information systems not being properly managed throughout their lifecycle and that new projects will fail to meet the stated objectives and budgets.

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."

Recommendation 3 (*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. During transitions of two CIO's since the prior recommendation, it was decided to update the SDLC into a Digital Transformation SDLC during FY 2017. This will be a collaborative effort between OPM SDLC Owner and the

18F team that is working with OPM. This SDLC will be completed with an initial iteration and expanded upon with each successive project that transforms to agile development processes."

B. Security Assessment and Authorization

An Information System Security Assessment and Authorization (Authorization) is a comprehensive assessment that evaluates whether a system's security controls are meeting the security requirements of that system.

OPM is working to implement a comprehensive security control continuous monitoring program that will eventually replace the need for periodic system Authorizations. Although the agency's continuous monitoring program is rapidly improving, it has not reached the point of maturity where it can effectively replace the Authorization program (See Section H - Continuous Monitoring). In addition, OPM acknowledges that a current and comprehensive Authorization for each system is a prerequisite for a continuous monitoring program, as the Authorization will provide a baseline of the security controls that need to be continuously monitored going forward.

Our previous FISMA audit reports identified a material weakness in OPM's Authorization program related to incomplete, inconsistent, and sub-par Authorization 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 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 the end of FY 2016. All new Authorization activity was deferred. 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.

Although the moratorium on Authorizations has since been lifted, the effects of the April 2015 memorandum continue to have a significant negative impact on the agency. The infrastructure modernization project was suspended as the agency re-evaluates its approach, and many of the systems included in the memorandum continue to operate in the same legacy environment without a valid Authorization.

In FY 2016, OPM initiated an "Authorization Sprint" in an effort to get all of the agency's systems compliant with the Authorization requirements. We acknowledge that OPM is once again taking system Authorization seriously, and is dedicating significant resources toward re-Authorizing the systems that were neglected as a result of the 2015 moratorium. However, the ISSO staffing issues discussed in section A, above, are preventing OPM from moving as quickly as it would like. In FY 2016, we have received evidence that 12 systems were subject to the Authorization process as part of the Authorization Sprint. This includes an Authorization for OPM's "LAN/WAN," which is a critical general support system that provides inheritable controls for many smaller applications. The OIG was provided many of these Authorization packages during the last two weeks of the fiscal year, and therefore we were unable to perform a comprehensive review of the content and quality of these packages before issuing this FY 2016 FISMA audit report. We will perform a comprehensive audit of OPM's Authorization process as a whole in early FY 2017.

Although OPM has put significant effort toward authorizing its information systems, there are still 18 major systems that do not have a current Authorization in place. This includes systems owned by the following program offices:

- Chief Financial Officer (2 system);
- Chief Information Officer (5 systems);
- Employee Services (1 system);
- Federal Investigative Services (4 systems)[1];
- Human Resources Solutions (1 system);
- Office of the Inspector General (1 system); and
- Retirement Services (4 systems).

OPM is taking steps to improve its Authorization process, but it continued to represent a material weakness at the end of FY 2016.

NIST SP 800-53, Revision 4, states that an organization is to ensure "that the authorizing official authorizes the information system for processing before commencing operations; and … Updates the security authorization …."

While we acknowledge OPM's ongoing efforts to address this issue, we believe that the volume and sensitivity of OPM systems that are currently operating without an active Authorization continues to represent a material weakness in the internal control structure of the agency's IT security program.

Recommendation 4 ***(Rolled Forward from 2014)***

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

[1] As of October 1, 2016, the responsibilities of the Federal Investigative Services program office were transitioned to the National Background Investigation Bureau.

OPM Response:

"We concur with the recommendation. In FY 2016, OPM issued 15 ATOs during its ATO sprint and ATO relay initiatives and has 7 more authorizations in progress. OCIO plans to have current ATOs for all systems by December 31, 2016."

Recommendation 5 ***(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 concur with the recommendation. OCIO established and implemented these performance standards for the OCIO IT Project managers in FY 2015. In FY 2017, OCIO will develop the performance standards for all IT Program and Project Managers in coordination with the OPM Chief Human Capital Officer as required in the Federal IT Acquisition Reform Act implementation memo signed by the Acting Director in October 2016."

Recommendation 6 ***(Rolled Forward from 2014)***

We recommend that the OPM Director consider shutting down information systems that do not have a current and valid Authorization.

OPM Response:

"We partially concur with the recommendation. OCIO will update its policies and procedures for security authorizations to include making a risk-based decision on the operation of a system without a current authorization. These will be forwarded to the Director for ultimate decision."

OIG Comment:

Our recommendation is for the Director to *consider* shutting down systems that do not have a valid Authorization, and it appears that OPM's action plan is consistent with this recommendation. Once the relevant policies and procedures are updated, OPM should provide evidence to its IOC division for consideration of closing this recommendation.

C. Risk Management

NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems" (Guide) provides Federal agencies with a framework for implementing an agency-wide risk management methodology. The Guide suggests that risk be assessed in relation to the agency's goals and mission from a three-tiered approach:

- Tier 1: Organization (Governance);
- Tier 2: Mission/Business Process (Information and Information Flows); and
- Tier 3: Information System (Environment of Operation).

NIST SP 800-39, "Managing Information Security Risk – Organization, Mission, and Information System View" provides additional details of this three-tiered approach.

1) Agency Risk Management

NIST SP 800-39 states that agencies should establish and implement "Governance structures [that] provide oversight for the risk management activities conducted by organizations and include:

(i) the establishment and implementation of a *risk executive (function)*;
(ii) the establishment of the organization's risk management strategy including the determination of *risk tolerance*; and
(iii) the development and execution of organization-wide *investment strategies* for information resources and information security."

In FY 2016, OPM created a charter for a Risk Steering Committee, and the committee has begun to meet. However, OPM has not established an agency-wide risk management strategy. In addition, the 12 primary elements of the Risk Executive Function as described in NIST SP 800-39 are not all fully implemented. Key elements still missing from OPM's approach to managing risk at an agency-wide level include: conducting an agency-wide risk assessment, maintaining a risk registry, communicating the agency-wide risks down to the system owners, and ensuring proper authorization of agency information systems.

Recommendation 7 (*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. Responsibility for the development and maintenance of the enterprise risk management program was assigned to the Risk Management Council (RMC) in October 2015. As noted in NIST 800-39, 'the risk executive (function) requires a mix of skills, expertise, and perspectives to understand the strategic goals and objectives of organizations, organizational missions/business functions, technical possibilities and constraints, and key mandates and guidance that shape organizational operations.' To provide this necessary mixture, we will fill the risk executive (function) through the RMC. The Council is working toward meeting all requirements, with the OCIO specifically managing risk associated with the IT portfolio."

2) System Specific Risk Management

NIST SP 800-37, Revision 1, outlines a risk management framework (RMF) that contains six primary steps, including "(i) the categorization of information and information systems; (ii) the selection of security controls; (iii) the implementation of security controls; (iv) the assessment of security control effectiveness; (v) the authorization of the information system; and (vi) the ongoing monitoring of security controls and the security state of the information system."

OPM has implemented the six-step RMF into its system-specific risk management activities through the Authorization process (See Security Assessment and Authorization section B). In addition, OPM policy requires each major information system to be subject to routine security controls testing through a continuous monitoring program (see Continuous Monitoring section G).

3) Adherence to Remediation Deadlines

Many information system owners are not meeting the self-imposed deadlines for remediating the security weaknesses listed on the Plan of Action and Milestones (POA&M). Of OPM's 46 major information systems, 43 have POA&M items that are greater than 120 days overdue. Furthermore, 85 percent of open POA&Ms are over 30 days overdue, and over 78 percent are over 120 days overdue. The 43 systems with overdue POA&M items are owned by the following program offices:

- Chief Information Officer (10 systems);
- Employee Services (2 systems);
- Federal Investigative Services (8 systems);

- Healthcare and Insurance (3 systems);
- Human Resources Solutions (8 systems);
- Leadership and Talent Management (2 systems);
- Office of the Inspector General (3 systems);
- Planning and Policy Analysis (1 system); and
- Retirement Services (6 systems).

78 percent of all POA&Ms agency-wide are over 120 days overdue.

Recommendation 8

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

OPM Response:

"We concur with the recommendation. An updated POA&M guide and POA&M processes have been introduced in order to facilitate greater transparency of POA&M remediation actions and support more timely remediation through communication and mutual support amongst System Owners, Information System Security Officers, and other stakeholders in POA&M processes."

D. Contractor Systems

OPM's master system inventory indicates that 16 of the agency's 46 major applications are operated by a contractor.

OPM tracks interfaces between agency-operated and contractor-operated systems and the related Interconnection Security Agreements (ISA). However, the ISAs for 64 of the 82 interconnections have expired. NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, states that improperly designed interconnections could result in security failures that compromise the connected systems and the data that they store, process, or transmit. Failure to maintain valid ISAs could introduce risks similar to improperly designed interconnections.

Program offices may also develop a Memorandum of Understanding/Agreement (MOU/A) to document the purpose for direct interconnection. These documents outline the terms and conditions for sharing data and information resources in a secure manner. While these documents are not required for each ISA, OPM has created 28 MOU/As. However, 21 of those 28 MOU/As are expired. The OCIO should maintain up-to-date MOU/As to ensure that valid agreements are in place for each documented ISA.

Recommendation 9 (*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. OCIO will issue an updated policy on system interconnection requirements in the first quarter FY 2017. It will include monitoring processes for validating compliance with the policy."

Recommendation 10 (*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. OCIO will issue an updated policy on system interconnection requirements in the first quarter FY 2017. It will include monitoring processes for validating compliance with the policy."

E. Configuration Management

The sections below detail the controls that the OCIO has in place to manage the technical configuration of OPM servers, databases, and workstations.

1) Agency-wide Configuration Management Program

OPM's Information Security and Privacy Policy Handbook contains policies related to agency-wide configuration management. The handbook requires the establishment of secure baseline configurations and the monitoring and documenting of all configuration changes. Operational procedures are developed by individual program offices and technical operational groups as necessary.

2) System Inventory

OPM currently has several initiatives underway to improve its hardware and software inventory management program. The agency has recently made progress developing a list of its servers and databases, and uses an inventory management tool to track the software that is installed throughout the network.

However, lists of servers, databases, and software are only partial elements of a complete system inventory. OPM still has significant work ahead in converting the raw data it has collected into a comprehensive and mature system inventory. The current inventory data lists the devices and software that reside within the environment, but it does not describe the specific servers the software resides on, or the information systems the devices and software support.

The various elements of an inventory must be mapped to each other so that OPM can accurately define the boundaries of its information systems. A mature system inventory would not only identify all major information systems, but it would also contain details of the specific applications, software, servers, databases, and network devices that comprise and/or support each system. Furthermore, we issued a separate audit report on web application security that contained a recommendation related to OPM's lack of an adequate web application inventory.

The lack of a mature system inventory significantly hinders OPM's efforts related to oversight, risk management, and securing the agency's information systems.

Recommendation 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.

OPM Response:

"We concur with the recommendation. System Owners, Information System Security Officers, and Asset Managers will correlate hardware and software assets in the automated asset inventory to information systems in the information system inventory."

3) Standard Security Configurations Settings

Our FY 2015 FISMA audit concluded that OPM did not have adequate configuration standards in place for all operating platforms that it uses. In FY 2016, OPM developed an inventory of servers, databases, and applications – a critical first step toward developing security configurations standards. The agency has also begun using configuration checklists from recognized industry organizations to help develop the agency's standard security configuration settings. However, we have not seen evidence that these standards have been developed and implemented for all operating systems identified in the inventory.

In addition to not having documented configuration standards for some systems, OPM has not documented its deviations from generic standards for all operating systems in the environment. OPM requires all configuration deviations to be reviewed through the change control process. However, once they are approved, these settings must be documented in the appropriate standard.

NIST SP 800-53, Revision 4, requires agencies to identify, document, and approve any deviations from established configuration settings.

Configuration standards are the foundation of a mature configuration management program, as system configuration settings cannot be effectively monitored, audited, and secured without a documented standard to reference.

Recommendation 12 ***(Rolled Froward from 2014)***

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], [redacted], [redacted], and [redacted].

OPM Response:

"We partially concur with the recommendation. OCIO has baselines standardized across the infrastructure for the current approved operating platforms. Legacy systems (e.g. unsupported operating systems), with older, documented baselines continue to exist in the environment. OCIO will continue to strengthen its IT infrastructure environment by using only current, approved operating platforms with standard baseline configurations meeting the requirements defined in OPM security policies and procedures."

OIG Comment:

We have not been provided evidence that documented baselines exist for all legacy systems. If they do exist, evidence should be provided to the IOC division for consideration of closing this recommendation.

Recommendation 13 ***(Rolled Froward from 2014)***

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.

OPM Response:

"We partially concur with the recommendation. Although all changes to standard baselines are maintained and tracked as part of the Change Management process, OCIO realizes the value of maintaining a record specifically of the deviations to the standard baseline and will consider updating its standard baselines to include this information in accordance with security policies and standard best practices."

OIG Comment:

Maintaining a record of the specific deviations from generic configuration standards is critical to the organization's ability to effectively audit a system's actual settings. We continue to recommend that OPM document all instances where an OPM-specific configuration standard deviates from a generic recommended standard.

4) Vulnerability Management Program

OPM performs automated network vulnerability scans on its systems on a bi-weekly basis. The recent improvements to the agency's system inventory provide some level of confidence that the automated tools are actually scanning all systems within the environment.

OPM's vulnerability scanning program has recently improved, but our audit test work indicated that several problems still exist.

While we acknowledge that improvements have been made to OPM's vulnerability scanning program, our test work performed during this audit indicates that several problems still exist. Specifically, the scanning tool did not have access to certain portions of OPM's internal network. In some cases, OPM was not aware of these access issues until they were identified by our test work. In addition, the historical scan reports that we reviewed indicate that most of the vulnerability scans performed in the first half of the fiscal year were not run with the system credentials necessary to perform a thorough analysis.

We also performed our own independent vulnerability scans on a sample of OPM's information systems. The results of our vulnerability scans indicate that OPM's production environment contains severely out-of-date and 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 vulnerabilities that could be exploited to allow unauthorized access to sensitive data.

Recommendation 14 (*Rolled Forward from 2014*)

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

OPM Response:

"As noted in the report, OCIO encountered authentication errors in vulnerability scans and worked swiftly to formulate a remediation process. Procedures were updated to perform checks against authentication failures against the prior day's scheduled scans. OCIO now regularly runs discovery scans in order to identify any devices that are connected to the opm.gov network. We believe that these updated procedures address the recommendation."

OIG Comment:

As part of the audit resolution process, we recommend that OPM provide its IOC division with evidence that all network devices have been routinely subject to authenticated vulnerability scans over a six-month period.

Recommendation 15

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. In FY 2016, OCIO implemented a Network Access Control (NAC) solution across the enterprise to prevent unauthorized operating platforms from accessing the network environment. The NAC also monitors systems to ensure they are in compliance with NAC security policies. OCIO has also implemented additional tools as part of the CDM effort, including a software 'Blacklist,' and is working to implement 'Whitelisting' into FY 2017. OCIO has also reduced the number of unsupported [redacted] operating platforms in its environment by 93% in FY 2016 and plans to complete these upgrades in FY 2017. OPM project managers and security officers will work with business owners to implement good software lifecycle practices across the agency and migrate from unsupported applications and operating platforms to current versions."

5) Compliance with Baselines

OPM uses automated scanning tools to conduct routine configuration compliance audits on its workstations, servers, and networking devices. These tools compare the actual configuration settings to industry standard templates. However, these automated scans do not take into account the customized configuration requirements specific to OPM's technical environment. As mentioned above, OPM does not maintain documented configuration standards that detail these customizations, and therefore it is impossible to subject these systems to adequate configuration compliance audits.

NIST SP 800-128 states that configuration monitoring is needed to identify "undiscovered/undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes, all of which, if not addressed, can expose organizations to increased risk."

Failure to routinely audit information systems against their approved configurations decreases an organization's ability to detect malicious activity or unapproved changes.

Recommendation 16 ***(Rolled Forward from 2014)***

We recommend the OCIO conduct routine compliance scans against established baseline configurations for all servers and databases in use by OPM. *This recommendation cannot be addressed until Recommendation 13 has been completed.*

OPM Response:

"We concur with the recommendation. OCIO currently runs daily compliance scans against all established baselines through the use of OPM's enterprise compliance scanning tool. OCIO will continue to refine its enterprise compliance scanning tool to evaluate compliance against the established baselines as they are developed for the remaining servers and databases."

6) Vulnerability remediation

OPM distributes vulnerability scan results to the agency's 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, for other routine security weaknesses identified during vulnerability scans, OPM does not have a process to record or track the remediation status.

Without a formal process to track known vulnerabilities, there is a significantly increased risk that these weaknesses will not be addressed in a timely manner, and that the systems will indefinitely remain susceptible to attack.

OPM does not formally track known vulnerabilities, increasing the risk the systems will indefinitely remain susceptible to attack.

Recommendation 17 ***(Rolled Forward from 2014)***

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

OPM Response:

"We concur with the recommendation. OCIO will integrate the weaknesses identified through the vulnerability scanning process with the POA&M inventory for centralized tracking of security weaknesses."

7) Patch management

OPM has a process in place for testing and installing patches for each operating system used within OPM's network. The OCIO has been transitioning some of the patching process to a new management utility, but not all systems and applications are integrated at this time. The servers that have not been integrated with this new utility are patched via other utilities or manual processes.

We made various efforts to validate the effectiveness of the OCIO's patch management process – both by performing our own independent vulnerability scans and by reviewing the results of historical vulnerability scans run by OPM. However, these efforts did not produce any evidence indicating that OPM's systems are consistently patched in a timely manner. Although we acknowledge that OPM is dedicating resources to improving its patch management process, we cannot at this time attest to any significant improvements in OPM's patch management process and therefore, our previous recommendation on this issue will be rolled forward in this report.

Recommendation 18 ***(Rolled Forward from 2014)***

We recommend that the OCIO implement a process to apply operating system and third party vendor patches in a timely manner, which is defined within the OPM Information Security and Privacy Policy Handbook.

OPM Response:

"We concur with the recommendation. A new patch management application was implemented across the enterprise and has been used to patch systems for about six months. It has also successfully deployed software upgrades to the end-users workstations using current processes. OCIO will continue to refine the patch management process using this application into FY 2017."

F. Identity and Access Management

The following sections detail OPM's account and identity management program.

a) Policies for account and identity management

OPM maintains policies and procedures for agency-wide system account and identity management within its Information Security and Privacy Policy Handbook. The policies contain procedures for creating user accounts with the appropriate level of access as well as procedures for removing access for terminated employees.

b) Contractor Access Termination

OPM has established a centralized process for securely granting employees and contractors access to its internal network. Our evaluation of OPM's termination process indicates that the process appears to work as intended for removing terminated agency (non-contractor) employees in a timely manner. However, the process for terminating access for contractor employees 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.

FISCAM states that "Terminated employees who continue to have access to critical or sensitive resources pose a major threat . . . ."

Recommendation 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.

OPM Response:

"We partially concur with the recommendation. OCIO maintains a list of all employee and contractor accounts granting access to the OPM network; however, management of the OPM contractor workforce is an agency-wide effort. OCIO will engage appropriate program offices to support the management of contractor personnel. OCIO will review and update its account management processes to ensure network accounts are secured after contractor termination actions are taken in a timely manner in accordance with OPM security policies."

OIG Comment:

OPM's response states that it only partially concurs with the recommendation, but its action plan appears to be fully consistent with the original recommendation.

c) Multi-factor authentication with PIV

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

OPM-issued workstations can only be connected to the OPM network via two-factor authentication using PIV cards. In early FY 2016, OPM implemented controls that prevent non-OPM issued devices from connecting to the network. These controls close a previous loophole that allowed users to gain access to the network without PIV authentication. As such, OPM has successfully implemented a methodology that requires all users to connect to the network using PIV authentication.

Only 2 of OPM's 46 major applications are compliant with OMB requirements related to PIV authentication.

Although OPM has made progress in requiring PIV authentication to gain access to the network, this does not fully satisfy OMB mandates related to two-factor authentication. OMB Memorandum M-11-11 states that PIV credentials must be used to gain authorized access to an agency's 1) facilities, 2) network, and 3) information systems. OPM is not fully PIV compliant until all of its information systems (applications) can be accessed only via PIV authentication in lieu of a username and password. Our audit work indicated that only 2 of OPM's 46 major applications enforced PIV authentication. This is a critical control because without PIV authentication enforced at the application level, users of the network (either authorized or

unauthorized) could still gain access to applications that they are not authorized to use, and public-facing systems are more vulnerable to remote attack.

Recommendation 20 ***(Rolled Forward from 2012)***

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

OPM Response:

"We concur with the recommendation. In FY 2016, OCIO initiated a project to implement an enterprise Identity and Access Management (IDAM) solution to manage access to OPM systems for both internal users and external customers. OCIO will continue its work on this project for enforcing multi-factor authentication, including the use of PIV credentials wherever feasible and appropriate."

d) Securing Public Websites

In FY 2016, we evaluated OPM's efforts to implement Hyper Text Transport Protocol Secure (HTTPS) on all of its publicly accessible websites, as required by OMB Memorandum M-15-13. We issued a memorandum to the OCIO to communicate the results of our evaluation on February 25, 2016. Our evaluation indicated that only a small percentage of OPM's publicly accessible websites were compliant with the regulation – which requires full implementation by December 31, 2016.

In recent months, however, OPM has made a significant effort to improve its compliance. OPM has stated that 47 of the 60 websites are now compliant, but we have not confirmed this. We will continue to monitor OPM's progress with implementing the requirements outlined in OMB memorandum M-15-13 and will perform additional tests once OPM believes that it is 100 percent compliant.

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 additional specialized training.

a) IT security awareness training

The OCIO provides annual IT security and privacy awareness training to all OPM employees 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 94 percent of OPM's employees and contractors completed the security awareness training course in FY 2016.

b) Specialized IT security training

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 for specific job roles. The OCIO uses a spreadsheet to track the security training taken by employees that have been identified as having security responsibility. Only 73 percent of employees identified as having significant security responsibilities completed specialized IT security training in FY 2016.

Recommendation 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.

OPM Response:

"We concur with the recommendation. OCIO has updated its Security Awareness and Training policy, reinforcing the training requirements, and is tracking progress toward completion."

H. Continuous Monitoring

The following sections detail our review of OPM's efforts to continuously monitor the security controls of its information systems.

a) Information Security Continuous Monitoring Program

In FY 2015, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed a Continuous Monitoring Maturity Model that provides a framework for evaluating an agency's information security program and ranking the maturity of its

security control monitoring program on a five-level scale (level one being the least mature and effective, five being completely mature).

We used this maturity model to conduct a review of OPM's information systems continuous monitoring program (ISCM). Our review determined that OPM's ISCM is currently operating at level 2, "Defined." This is an improvement from the prior year, as our FY 2015 FISMA audit report had previously evaluated the ISCM program at level 1, "Ad Hoc."

In FY 2016, OPM developed a new set of policies and procedures for the agency's ISCM program. These policies and procedures included the necessary controls required by CIGIE's ISCM maturity model.

The development of these new policies and procedures is a step in the right direction towards a mature ISCM program. However, OPM still has a significant amount of work to complete before it reaches the next level (level three, "Consistently Implemented") of the ISCM maturity model. We provided the OCIO with a listing of the specific ISCM elements that it must implement to reach level three of the maturity model.

During this fiscal year the OCIO also acquired a new software tool that will better support the requirements of the ISCM program. However, the OCIO has not fully implemented this tool in this fiscal year. The use of the technology and automated tools to support a continuous monitoring program is a critical element of CIGIE's ISCM Maturity Model.

As previously discussed in the information security governance section above, OPM's ISSO positions are severely understaffed, and these individuals have multiple responsibilities within the ISCM program. We believe that the staffing limitations are having a negative impact on OPM's ability to implement a more mature continuous monitoring program.

Recommendation 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."

OPM Response:

"We partially concur with the recommendation. OCIO is hiring ISSOs to support the information security continuous monitoring (ISCM) program in order to provide adequate support for all OPM information systems, and integrate the automated tools it has deployed in FY 2016 under the Continuous Diagnostics and Mitigation program. OPM appreciates the value of a maturity model as a means to uniformly evaluate agencies against standard criteria for the ISCM program. OPM will continue to implement the ISCM program in accordance with Federal policy and NIST standards and guidelines."

OIG Comment:

The CIGIE ISCM maturity model is in line with Federal policy and NIST standards, therefore OPM's ongoing efforts to meet these requirements will ultimately address this audit recommendation.

b) Assessment of Individual System Security Controls

Since OPM's continuous monitoring program is not fully matured, we continue to expect the agency to manually assess the security controls of each information system on a routine basis. 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 current policy requires the owners of all OPM-operated system to submit evidence of ongoing security control testing activity at least quarterly. Security control testing is currently only required annually for OPM systems operated by a contractor.

We requested the security control testing documentation for all OPM systems in order to review them for quality and consistency. We determined that only 16 of OPM's 46 systems were subject to adequate security control testing activity in FY 2016.

The following program offices own information systems that failed the security control testing requirements in FY 2016:

- Chief Financial Officer (1 system);
- Chief Information Officer, CIO (5 systems);
- Employee Services (1 system);
- Federal Investigative Services (8 systems);
- Human Resources Solutions (8 systems);
- Planning and Policy Analysis (1 system); and
- Retirement Services (6 systems).

It has been over 10 years since all OPM systems were subject to an adequate security controls test within a single fiscal year.

Failure to continuously monitor and assess security controls increases the risk that agency officials are unaware of major risks that exist within the organization.

It has been over 10 years since all OPM systems were subject to an adequate security controls test within a single fiscal year.

Recommendation 23 (*Rolled forward from 2008*)

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

OPM Response:

"We concur with the recommendation. OCIO is hiring the necessary ISSOs to support annual security control testing for all information systems in accordance with OPM continuous monitoring policies and procedures."

I. Incident Response Program

In FY 2016, the CIGIE developed an Incident Response Program Maturity Model that provides a framework for evaluating an agency's cyber defense program and ranking the maturity of its incident response handling procedures on a five-level scale (level one being the least mature and effective, five being completely mature).

We used this maturity model to review OPM's incident response program. Our review determined that OPM's incident response program is currently operating at level 2, "Defined." In FY 2016, the OCIO completed a new set of policies and procedures for the agency's incident response program. These policies and procedures addressed the necessary controls identified in CIGIE's incident response program maturity model.

The OCIO has recently made significant improvements in its cyber defense program and has actually implemented the majority of the requirements to reach level three of the incident response maturity model. Most notably, OPM has implemented automated tools used to develop and maintain a baseline of network operations and expected data flows for information systems. However, agencies must meet 100 percent of the elements of each maturity model level before being rated at that level. We provided the OCIO with a listing of the specific incident response program elements that it must implement to reach level three of the maturity model.

Recommendation 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."

OPM Response:

"We partially concur with the recommendation. OCIO provided a Cyber Protection and Defense Manual during the course of the audit that defined many of the requirements described within the maturity model. OCIO will follow up on any identified gaps in its TIC security controls as identified by DHS and continue to evaluate capabilities for defining expected data flows for users and systems. OPM appreciates the value of a maturity model as a means to uniformly evaluate agencies against standard criteria for the incident response program. OPM will continue to implement the incident response program in accordance with Federal policy and NIST standards and guidelines."

OIG Comment:

The CIGIE incident response maturity model is consistent with Federal policy and NIST standards, therefore OPM's ongoing efforts to meet these requirements will ultimately address this audit recommendation.

J. Contingency Planning

OPM's Information Security Privacy and Policy Handbook requires a contingency plan to be in place for each information system and that each system's contingency plan be tested on an annual basis. The sections below detail our review of contingency planning activity in FY 2016.

1) Maintaining Contingency Plans

We received contingency plans for 45 of 46 OPM major systems. However, only 17 of the plans received had been reviewed within the current fiscal year. Therefore, we do not believe that these documents have been adequately maintained and updated, as they do not contain current information regarding the impact that the ongoing changes to OPM's infrastructure have to the system's contingency plan. Maintaining an up-to-date contingency plan is a critical element to ensuring information systems can be properly recovered in the event of an emergency or disaster.

The Information Security Privacy and Policy Handbook states that OPM system owners "shall ensure the establishment, maintenance, and effective implementation of plans for emergency response, disaster recovery, backup operations, and post-disaster recovery for their information systems . . . ."

Recommendation 25 ***(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. With the ISSOs in place, OCIO will ensure system owners and project owners review and update their contingency plans annually."

b) Contingency Plan Tests

It has been over 9 years since the contingency plans for all OPM systems were tested within a single fiscal year.

OPM's Information Security Privacy and Policy Handbook obligates system owners to test or exercise each system's contingency plans at least annually. During the course of our audit we received evidence that only 2 of OPM's 46 major information systems were subject to an adequate contingency plan test in FY 2016. Furthermore, 9 of the 46 major systems have not been tested at all since 2014. These 9 systems are owned by:

- Employee Services (2 systems);
- Federal Investigative Services (4 systems);
- Healthcare and Insurance Federal Employee Insurance Operations (1 system); and
- Retirement Services (2 systems).

Recommendation 26 ***(Rolled Forward from 2008)***

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

OPM Response:

"We concur with the recommendation. With the ISSOs in place, OCIO will ensure system owners and project owners will test contingency plans annually."

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], Lead IT Auditor-In-Charge
[redacted], Senior Team Leader
[redacted], IT Auditor
[redacted], IT Auditor
[redacted], IT Auditor
[redacted], IT Auditor

[redacted], Group Chief

Appendix I

The tables below outline the current status of prior audit recommendations issued in FY 2015 by the Office of the Inspector General.

Report No. 4A-CI-00-15-011: FY 2015 Federal Information Security Management Act Audit, issued November 10, 2015

Rec #	Original Recommendation	Recommendation History	Current Status
1	We recommend that the OCIO develop and maintain a comprehensive inventory of all servers, databases, and network devices that reside on the OPM network.	Rolled forward from FY 2014	CLOSED 7/20/16
2	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.	Rolled forward from FY 2013	OPEN: Rolled-forward as Report 4A-CI-00-16-039 Recommendation 3
3	We recommend that all active systems in OPM's inventory have a complete and current Authorization.	Rolled forward from FY 2014	OPEN: Rolled-forward as Report 4A-CI-00-16-039 Recommendation 4
4	We recommend that the performance standards of all OPM system owners be modified to include a requirement related to FISMA compliance for the information systems they own. At a minimum, system owners should be required to ensure that their systems have valid Authorizations.	Rolled forward from FY 2014	OPEN: Rolled-forward as Report 4A-CI-00-16-039 Recommendation 5
5	We recommend that the OPM Director consider shutting down information systems that do not have a current and valid Authorization.	Rolled forward from FY 2014	OPEN: Rolled-forward as Report 4A-CI-00-16-039 Recommendation 6
6	We recommend that the new ISCM policies and procedures being developed utilize and incorporate the controls identified in the CIGIE Information Security Continuous Monitoring Maturity Model. At a minimum the policies and procedures should:	New recommendation in FY 2015	CLOSED with issuance of Final Report 11/9/2016
7	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-00-16-039 Recommendation 23
8	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], [redacted], [redacted], and [redacted].	Rolled forward from FY 2014	OPEN: Rolled-forward as Report 4A-CI-00-16-039 Recommendation 12

9	We recommend the OCIO conduct routine compliance scans against established baseline configurations for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 8 has been completed.	Rolled forward from FY 2014	OPEN: Rolled-forward as Report 4A-CI-00-16-039 Recommendation 16
10	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-00-16-039 Recommendation 14
11	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-00-16-039 Recommendation 17
12	We recommend that the OCIO document "accepted" weaknesses identified in vulnerability scans.	Rolled forward from FY 2011	CLOSED: 3/01/2016
13	We recommend the OCIO implement a process to ensure that only supported software and operating platforms are utilized within the network environment.	New recommendation in FY 2015	OPEN: Rolled-forward as Report 4A-CI-00-16-039 Recommendation 15
14	We recommend 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-00-16-039 Recommendation 18
15	We recommend that the OCIO require PIV authentication to access the OPM network.	New recommendation in FY 2015	CLOSED 11/10/15
16	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-00-16-039 Recommendation 20
17	We recommend that OCIO configure its security information and event management tool to collect and report meaningful data, while reducing the volume of non-sensitive log and event data.	Rolled forward from FY 2014	CLOSED 11/10/15
18	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-00-16-039 Recommendation 7
19	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 2015	CLOSED: 11/20/15

20	We recommend that the OCIO and program offices that own information systems ensure that all known security weaknesses are incorporated into the appropriate POA&M.	Rolled forward from FY 2014	CLOSED: 12/18/15
21	We recommend that the OCIO and system owners develop formal corrective action plans to remediate all POA&M weaknesses that are over 120 days overdue.	New recommendation in FY 2015	CLOSED with issuance of Final Report 11/9/2016
22	We recommend that all POA&Ms list the specific resources required to address each security weakness identified.	New recommendation in FY 2015	CLOSED 1/6/16
23	We recommend the OCIO configure the VPN servers to terminate VPN sessions after 30 minutes of inactivity.	Rolled forward from FY 2012	CLOSED: 3/22/2016
24	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-00-16-039 Recommendation 25
25	We recommend that OPM's program offices test the contingency plans for each system on an annual basis. The contingency plans should be immediately tested for the 29 systems that were not subject to adequate testing in FY 2015.	Rolled forward from FY 2008	OPEN: Rolled-forward as Report 4A-CI-00-16-039 Recommendation 26
26	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-00-16-039 Recommendation 9
27	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-00-16-039 Recommendation 10

Appendix II

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Information Officer

MEMORANDUM FOR NICHOLAS HOYLE
CHIEF, INFORMATION SYSTEMS AUDIT GROUP
OFFICE OF THE INSPECTOR GENERAL

FROM: DAVID L. DEVRIES
CHIEF INFORMATION OFFICER

DAVID DEVRIES
Digitally signed by DAVID DEVRIES
Date: 2016.10.22 20:00:01 -04'00'

Subject: Office of the Chief Information Officer Response to the Office of the Inspector General Federal Information Security Modernization Act Audit – FY 2016 (Report No. 4A-CI-00-16-039)

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 help ensure we 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 help ensure we remain aligned.

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 the agency's major information systems.

Management Response: We concur with the recommendation. In FY 2016, OPM hired eight ISSOs bringing the total to 16 ISSOs currently in place. The Office of the Chief Information Officer (OCIO) is hiring an additional eight ISSOs, three of which are now onboarding, for a total of 24 ISSO positions, which will support all of OPM's major information systems.

Recommendation 2
We recommend that OPM thoroughly define the roles and responsibilities of all positions in its IT security management structure.

Management Response: We concur with the recommendation. OCIO is finalizing the updated IT security policies and procedures involving the positions within the IT security management structure in the OCIO, including updated roles and responsibilities.

Recommendation 3
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. During transitions of two CIO's since the prior recommendation, it was decided to update the SDLC into a Digital Transformation SDLC during FY 2017. This will be a collaborative effort between OPM SDLC Owner and the 18F team that is working with OPM. This SDLC will be completed with an initial iteration and expanded upon with each successive project that transforms to agile development processes.

Recommendation 4
We recommend that all active systems in OPM's inventory have a complete and current Authorization.

Management Response: We concur with the recommendation. In FY 2016, OPM issued 15 ATOs during its ATO sprint and ATO relay initiatives and has 7 more authorizations in progress. OCIO plans to have current ATOs for all systems by December 31, 2016.

Recommendation 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.

Management Response: We concur with the recommendation. OCIO established and implemented these performance standards for the OCIO IT Project managers in FY 2015. In FY 2017, OCIO will develop the performance standards for all IT Program and Project Managers in coordination with the OPM Chief Human Capital Officer as required in the Federal IT Acquisition Reform Act implementation memo signed by the Acting Director in October 2016.

Recommendation 6
We recommend that the OPM Director consider shutting down information systems that do not have a current and valid Authorization.

Management Response: We partially concur with the recommendation. OCIO will update its policies and procedures for security authorizations to include making a risk-based decision on the operation of a system without a current authorization. These will be forwarded to the Director for ultimate decision.

Recommendation 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).

Management Response: We concur with the recommendation. Responsibility for the development and maintenance of the enterprise risk management program was assigned to the Risk Management Council (RMC) in October 2015. As noted in NIST 800-39, "the risk executive (function) requires a mix of skills, expertise, and perspectives to understand the strategic goals and objectives of organizations, organizational missions/business functions, technical possibilities and constraints, and key mandates and guidance that shape organizational operations." To provide this necessary mixture, we will fill the risk executive (function) through the RMC. The Council is working toward meeting all requirements, with the OCIO specifically managing risk associated with the IT portfolio.

Note - draft recommendation 8 was deleted from the final audit report. Subsequent recommendations from the draft audit report were renumbered for the final audit report.

Recommendation 9
We recommend that OPM adhere to remediation dates for its POA&M weaknesses.

Management Response: We concur with the recommendation. An updated POA&M guide and POA&M processes have been introduced in order to facilitate greater transparency of POA&M remediation actions and support more timely remediation through communication and mutual support amongst System Owners, Information System Security Officers, and other stakeholders in POA&M processes.

Recommendation 10
We recommend that the OCIO ensure that all ISAs are valid and properly maintained.

Management Response: We concur with the recommendation. OCIO will issue an updated policy on system interconnection requirements in the first quarter FY 2017. It will include monitoring processes for validating compliance with the policy.

Recommendation 11
We recommend that the OCIO ensure that a valid MOU/A exists for every interconnection.

Management Response: We concur with the recommendation. OCIO will issue an updated policy on system interconnection requirements in the first quarter FY 2017. It will include monitoring processes for validating compliance with the policy.

Recommendation 12
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. System Owners, Information System Security Officers, and Asset Managers will correlate hardware and software assets in the automated asset inventory to information systems in the information system inventory.

Recommendation 13
We recommend that the OCIO implement configuration baselines for all operating platforms in use by OPM.

Management Response: We partially concur with the recommendation. OCIO has baselines standardized across the infrastructure for the current approved operating platforms. Legacy systems (e.g. unsupported operating systems), with older, documented baselines continue to exist in the environment. OCIO will continue to strengthen its IT infrastructure environment by using only current, approved operating platforms with standard baseline configurations meeting the requirements defined in OPM security policies and procedures.

Recommendation 14
In instances where a configuration standard is based on a pre-existing standard, we recommend that OPM document all instances where the OPM-specific standard deviates from the recommended configuration setting.

Management Response: We partially concur with the recommendation. Although all changes to standard baselines are maintained and tracked as part of the Change Management process, OCIO realizes the value of maintaining a record specifically of the deviations to the standard baseline and will consider updating its standard baselines to include this information in accordance with security policies and standard best practices.

Recommendation 15
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: As noted in the report, OCIO encountered authentication errors in vulnerability scans and worked swiftly to formulate a remediation process. Procedures were updated to perform checks against authentication failures against the prior day's scheduled scans. OCIO now regularly runs discovery scans in order to identify any devices that are connected to the opm.gov network. We believe that these updated procedures address the recommendation.

Recommendation 16
We recommend that the OCIO implement a process to ensure that only supported software and operating platforms are utilized within the network environment.

Management Response: We concur with the recommendation. In FY 2016, OCIO implemented a Network Access Control (NAC) solution across the enterprise to prevent unauthorized operating platforms from accessing the network environment. The NAC also monitors systems to ensure they are in compliance with NAC security policies. OCIO has also implemented additional tools as part of the CDM effort, including a software ‘Blacklist,’ and is working to implement ‘Whitelisting’ into FY 2017. OCIO has also reduced the number of

unsupported [redacted] operating platforms in its environment by 93% in FY 2016 and plans to complete these upgrades in FY 2017. OPM project managers and security officers will work with business owners to implement good software lifecycle practices across the agency and migrate from unsupported applications and operating platforms to current versions.

Recommendation 17
We recommend the OCIO conduct routine compliance scans against established baseline configurations for all servers and databases in use by OPM. *This recommendation cannot be addressed until Recommendation 13 has been completed.*

Management Response: We concur with the recommendation. OCIO currently runs daily compliance scans against all established baselines through the use of OPM's enterprise compliance scanning tool. OCIO will continue to refine its enterprise compliance scanning tool to evaluate compliance against the established baselines as they are developed for the remaining servers and databases.

Recommendation 18
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 will integrate the weaknesses identified through the vulnerability scanning process with the POA&M inventory for centralized tracking of security weaknesses.

Recommendation 19
We recommend 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.

Management Response: We concur with the recommendation. A new patch management application was implemented across the enterprise and has been used to patch systems for about six months. It has also successfully deployed software upgrades to the end-users workstations using current processes. OCIO will continue to refine the patch management process using this application into FY 2017.

Recommendation 20
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 partially concur with the recommendation. OCIO maintains a list of all employee and contractor accounts granting access to the OPM network; however, management of the OPM contractor workforce is an agency-wide effort. OCIO will engage appropriate program offices to support the management of contractor personnel. OCIO will review and update its account management processes to ensure network accounts are secured after contractor termination actions are taken in a timely manner in accordance with OPM security policies.

Recommendation 21
We recommend that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.

Management Response: We concur with the recommendation. In FY 2016, OCIO initiated a project to implement an enterprise Identity and Access Management (IDAM) solution to manage access to OPM systems for both internal users and external customers. OCIO will continue to its work on this project for enforcing multi-factor authentication, including the use of PIV credentials wherever feasible and appropriate.

Recommendation 22
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.

Management Response: We concur with the recommendation. OCIO has updated its Security Awareness and Training policy, reinforcing the training requirements, and is tracking progress toward completion.

Recommendation 23
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".

Management Response: We partially concur with the recommendation. OCIO is hiring ISSOs to support the information security continuous monitoring (ISCM) program in order to provide adequate support for all OPM information systems, and integrate the automated tools it has deployed in FY 2016 under the Continuous Diagnostics and Mitigation program. OPM appreciates the value of a maturity model as a means to uniformly evaluate agencies against standard criteria for the ISCM program. OPM will continue to implement the ISCM program in accordance with Federal policy and NIST standards and guidelines.

Recommendation 24
We recommend that OPM ensure that an annual test of security controls has been completed for all systems.

Management Response: We concur with the recommendation. OCIO is hiring the necessary ISSOs to support annual security control testing for all information systems in accordance with OPM continuous monitoring policies and procedures.

Recommendation 25
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".

Management Response: We partially concur with the recommendation. OCIO provided a Cyber Protection and Defense Manual during the course of the audit that defined many of the requirements described within the maturity model. OCIO will follow up on any identified gaps

in its TIC security controls as identified by DHS and continue to evaluate capabilities for defining expected data flows for users and systems. OPM appreciates the value of a maturity model as a means to uniformly evaluate agencies against standard criteria for the incident response program. OPM will continue to implement the incident response program in accordance with Federal policy and NIST standards and guidelines.

Recommendation 26
We recommend that the OCIO ensures that all contingency plans are in place for OPM's major systems.

Management Response: We concur with the recommendation. With the ISSOs in place, OCIO will ensure system owners and project owners review and update their contingency plans annually.

Recommendation 27
We recommend that the OPM program offices test each contingency plan annually.

Management Response: We concur with the recommendation. With the ISSOs in place, OCIO will ensure system owners and project owners will test contingency plans annually.

Again, thank you for the opportunity to provide comment. Please contact me or [redacted] if you have questions or need additional information.

cc:
[redacted]
Chief Information Security Officer

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

Janet L. Barnes
Director, Internal Oversight and Compliance

Appendix III

Appendix III contains a system-generated report exported from the CyberScope FISMA Reporting Application. CyberScope is maintained by the U.S. Department of Homeland Security and the Office of Management and Budget.

The Office of the Inspector General at the U.S. Office of Personnel Management entered its fiscal year 2016 FISMA audit results and narrative comments into the CyberScope system. However, the numerical scores throughout the report were automatically generated by the system.

Inspector General

Section Report

2016

Annual FISMA

eport

Office of Personnel Managements

Section 0: Overall

0.1 Please provide an overall narrative assessment of the agency's information security program. 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 this response to conform with the grammatical and narrative structure of the Annual Report.

This audit rolls-forward a material weakness related to OPM's Security Assessment and Authorization (Authorization) program. At the end of fiscal year (FY) 2016, the Agency still had at least 18 major systems without a valid Authorization in place. However, OPM has recently placed significant effort toward meeting Authorization requirements. We intend to perform a comprehensive audit of OPM's Authorization process as a whole in early FY 2017.

This audit also re-opens a significant deficiency related to OPM's information security management structure. Although OPM ha developed a security management structure that we believe can be effective, there has been an extremely high turnover rate of critical positions. The negative impact of these staffing issues is apparent in the re ults of our current FISMA audit work. There has been a significant regre ion in OPM's compliance with FISMA equirements, as the agency failed to meet requirements that it had successfully met in prior year . We acknowledge that OPM has placed significant effort toward filling these positions, but simply having the staff on board does not guarantee that the team can effectively manage information security and keep OPM compliant with FISMA equirements. We will continue to closely monitor activity in this area throughout FY 2017.

Section 0: Overall

Comments: s

This audit rolls-forward a material weakness related to OPM's Security Assessment and Authorization (Authorization) program. In April 2015, the Chief Information Officer 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. Although the moratorium on Authorizations has since been lifted, the effects of the April 2015 memorandum continue to have a significant negative impact on OPM. At the end of fiscal year (FY) 2016, the Agency still had at least 18 major systems without a valid Authorization in place.

However, OPM initiated an "Authorization Sprint" in an effort to get all of the agency's systems compliant with the Authorization requirements. We acknowledge that OPM is once again taking system Authorization seriously. We intend to perform a comprehensive audit of OPM's Authorization process as a whole in early FY 2017.

This audit also re-opens a significant deficiency related to OPM's information security management structure. Although OPM has developed a security management structure that we believe can be effective, there has been an extremely high turnover rate of critical positions. The negative impact of these staffing issues is apparent in the results of our current FISMA audit work. There has been a significant regression in OPM's compliance with FISMA requirements, as the agency failed to meet requirements that it had successfully met in prior years. We acknowledge that OPM has placed significant effort toward filling these positions, but simply having the staff on board does not guarantee that the team can effectively manage information security and keep OPM compliant with FISMA requirements. We will continue to closely monitor activity in this area throughout FY 2017.

Section 1: Identify

Risk Management (Identify)s

1.1 Has the organization established a risk management program that includes comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**

Not Met

Comments: OPM has not developed a comprehensive list of agency policies and procedures consistent with FISMA requirements. In FY 2016 OPM began a process to update the information security policies for the agency, but these policies were not finalized during the fiscal year. OPM did not meet several additional FISMA risk management metrics this fiscal year.

1.1.1 Identifies and maintains an up-to-date system inventory, including organization- and contractor-operated systems, hosting environments, and systems residing in the public, hybrid, or private cloud. (2016 CIO FISMA Metrics, 1.1; NIST Cybersecurity Framework (CF) ID.AM.1, NIST 800-53: PM-5) **Defined**

Met

1.1.2 Develops a risk management function that is demonstrated throug the development, implementation, and maintenance of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, ev. 1. (NIST SP 800-39) **Consistently Implemented**

Not Met

Comments: In FY 2016, OPM created a charter for a Risk Steering Committee, and the committee has begun to meet. However, OPM has not established an agency-wide risk management strategy. In addition, the 12 primary elements of the Risk Executive Function as described in NIST SP 800-39 are not all fully implemented. Key elements still missing from OPM's approach to managing risk at an agency-wide level include: conducting an agency-wide risk assessment, maintaining a risk registry, communicating the agency-wide risks down to the system owners, and ensuring proper authorization of agency information systems.

1.1.3 Incorporates mission and business process-related risks into risk-based decisions at the organizational perspective, as described in NIST SP 800-37, Rev. 1. (NIST SP 800-39) **Consistently s Implementeds**

Not Met

Comments: As stated in metric 1.1.2 OPM currently operates without a proper risk governance structure and lower level risks are not incorporated into decisions at the organization level.

Section 1: Identify

1.1.4	Conducts information system level risk assessments that integrate risk decisions from the organizational and mission/business process perspectives and take into account threats, vulnerabilities, likelihood, impact, and risks from external parties and common control providers. (NIST SP 800-37, Rev. 1, NIST SP 800-39, NIST SP 800-53: RA-3) **Met**	**Consistently Implemented**
1.1.5	Provides timely communication of specific risks at the information system, mission/business, and organization-level to appropriate levels of the organization. **Not Met** **Comments:** There are currently no procedures to ensure that the Risk Steering committee provides sufficient communication of risks throughout the Agency.	**Managed and Measureable**
1.1.6	Performs comprehensive assessments to categorize information systems in accordance with Federal standards and applicable guidance. (FIPS 199, FIPS 200, FISMA, Cybersecurity Sprint, OMB M-16-04, President's Management Council (PMC) cybersecurity assessments) **Met**	**Consistently Implemented**
1.1.7	Selects an appropriately tailored set of baseline security controls based on mission/business requirements and policies and develops procedures to employ controls within the information system and its environment of operation. **Met**	**Defined**
1.1.8	Implements the tailored set of baseline security controls as described in 1.1.7. **Met**	**Consistently Implemented**
1.1.9	Identifies and manages risks with system interconnections, including through authorizing system interconnections, documenting interface characteristics and security requirements, and maintaining interconnection security agreements. (NIST SP 800-53: CA-3) **Not Met** **Comments:** OPM does not adequately authorize and document its system interconnections. Currently, 85 out of 110 Memorandums of Understanding and/or Interconnection Security Agreements documenting the agency's system interconnections have expired.	**Managed and Measureable**
1.1.10	Continuously assesses the security controls, including hybrid and shared controls, using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.	**Consistently Implemented**

Section 1: Identify

Not Mets

Comments:

OPM's continuous monitoring program is not fully matured, we therefore continue to expect the agency to manually assess the security controls of each information system on a routine basis. 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 current policy requires all OPM-operated system owners to submit evidence of ongoing security control testing activity on a quarterly basis. Security control testing is currently required only once a year for systems operated by a contractor. We determined that only 16 out of OPM's 46 systems were subject to adequate security control testing activity in FY 2016.

1.1.11 Maintains ongoing information system authorizations based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable (OMB M-14-03, NIST Supplemental Guidance on Ongoing Authorization).

Managed and s Measureables

Not Met

Section 1: Identify

Comments: s

OPM is working to implement a comprehensive security control continuous monitoring program that will eventually replace the need for periodic system Authorizations. Although the agency's continuous monitoring program is rapidly improving, it has not reached the point of maturity where it can effectively replace the Authorization program. In addition, OPM acknowledges that a current and comprehensive Authorization for each system is a prerequisite for a continuous monitoring program, as the Authorization will provide a baseline of the security controls that need to be continuously monitored going forward.

Our previous FISMA audit reports identified a material weakness in OPM's Authorization program related to incomplete, inconsistent, and sub-par Authorization 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 therefore we reinstated the material weakness related to this issue.

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 the end of FY 2016. The justification was that OPM was in the process of modernizing its IT infrastructure and that once this modernization is complete, 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.

Although the moratorium on Authorizations has since been lifted, the effects of the April 2015 memorandum continue to have a significant negative impact on the Agency. The infrastructure modernization project was suspended as the agency re-evaluates its approach, and many of the systems included in the memorandum continue to operate in the same legacy environment without a valid Authorization.

In FY 2016, OPM initiated an "Authorization Sprint" in an effort to get all of the agency's systems compliant with the Authorization requirements. We acknowledge that OPM is once again taking system Authorization seriously, and is dedicating significant resources toward re-Authorizing the systems that were neglected as a result of the 2015 moratorium.

Section 1: Identify

However the agency's ISSO staffing issues are preventing OPM from moving as quickly as it would like. In FY 2016, we have received evidence that 12 systems were subject to the Authorization process as part of the Authorization Sprint. This includes an Authorization for OPM's "LAN/WAN," which is a critical general support system that provides inheritable controls for many smaller applications. The OIG was provided many of these Authorization packages during the last two weeks of the fiscal year, and therefore we were unable to perform a comprehensive review of the content and quality of these packages before issuing the FY 2016 FISMA audit report. We will perform a comprehensive audit of OPM's Authorization process as a whole in early FY 2017.

1.1.12 Security authorization package contains system security plan, security assessment report, and POA&M that are prepared and maintained in accordance with government policies. (SP 800-18, SP_{800-37})

Managed and s Measureables

Met

1.1.13 POA&Ms are maintained and reviewed to ensure they are effective for correcting security weaknesses.

Consistently Implemented

Not Met

Comments:

Only 3 out of OPM's 46 major information systems do not have POA&M items that are greater than 120 days overdue. Furthermore, 85 percent of open POA&Ms are over 30 days or more$_{\text{overdue}}$, and over 78 percent are over 120 days overdue. As such we do not believe OPM is currently managing POA&Ms effectively to remediate weaknesses.

1.1.14 Centrally tracks, maintains, and independently reviews/validates POA&M activities at least quarterly. (NIST SP 800-53 :CA-5; OMB M-04-25)

Managed and Measureable

Met

1.1.15 Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information-system-related security risks.

Managed and Measureable

Not Met

Section 1: Identify

Comments:

OPM has designed (but not fully implemented) an information security management structure. One opportunity for improvement for this structure would be to more thoroughly define the roles and responsibilities of the individuals responsible for IT security and operations. Each ISSO position is complemented by an IT Project Manager (ITPM) position that typically has more operational (as opposed to security) responsibility. Throughout the fieldwork phase of this audit it became apparent to us that there is widespread confusion regarding whether certain responsibilities belong to the ISSO or the ITPM. One instance of this confusion came during our walkthrough of the vulnerability scanning process, where it was unclear to the individuals that received the scans results who would remediate and track the weaknesses identified. We understand that OPM is working on a draft document further defining the ISSO and ITPM roles and responsibilities, but it is still being developed and requires formal approval.

1.1.16 Implemented an insider threat detection and prevention program, including the development of comprehensive policies, procedures, guidance, and governance structures, in accordance with Executive Order 13587 and the National Insider Threat Policy. (PMC; NIST SP 800-53: PM-12)

Consistently s Implementeds

Met

1.1.17 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. Based on all testing performed, is the Risk Management program effective?

Not Effective

Comments:

Based on the volume and criticality of metrics in this section that were not met, we do not believe that OPM's risk management program is fully effective. However, we are optimistic that the agency appears to be taking steps to address the identified deficiencies.

Contractor Systems (Identify)

1.2 Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including other government agencies, managed hosting environments, and systems and services residing in a cloud external to the organization that is inclusive of policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?

Defined

Not Met

Section 1: Identify

Comments: OPM has not adequately established a program to oversee systems operated on its behalf by contractors or other entities, including other government agencies, managed hosting environments, and systems and services residing in a cloud external to the organization that is inclusive of policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. The vast majority of interconnection security agreements and memorandums of understanding related to contractor-operated system have expired.

1.2.1 Establishes and implements a process to ensure that contracts/statements of work/solicitations for systems and services, include appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information. (FAR Case 2007-004, Common Security Configurations, FA Sections 24.104, 39.101, 39.105, 39.106, 52.239-1; PMC, 2016 CIO Metrics 1.8, NIST 800-53, SA-4 FedRAMP standard contract clauses; Cloud Computing Contract Best Practices)

Consistently Implemented

Met

1.2.2 Specifies within appropriate agreements how information security performance is measured, reported, and monitored on contractor- or other entity-operated systems. (CIO and CAO Council Best Practices Guide for Acquiring IT as a Service, NIST SP 800-35)

Consistently Implemented

Not Met

Comments: s

OPM needs to ensure that valid MOUs and ISAs are implemented for all contractor systems.

1.2.3 Obtains sufficient assurance that the security controls of systems operated on the organization's behalf by contractors or other entities and services provided on the organization's behalf meet FISMA requirements, OMB policy, and applicable NIST guidelines. (NIST SP 800-53: CA-2, SA-9)

Consistently Implemented

Met

1.2.4 Provide any additional information on the effectiveness (positive or negative) of the organization's Contractor Systems Program that was not noted in the questions above. Based on all testing performed, is the Contractor Systems Program effective?

Not Effective

Comments: Based on the volume and criticality of metrics in this section that were not met, we do not believe that OPM's contractor system oversight program is fully effective. However, we are optimistic that the agency appears to be taking steps to address the identified deficiencies.

Level	Score	Possible Score
LEVEL 2: Defined	7	20

Section 2: Protect

Configuration Management (Protect)s

2.1 Has the organization established a configuration management program that is inclusive of comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**

Met

2.1.1 Develops and maintains an up-to-date inventory of the hardware assets (i.e., endpoints, mobile assets, network devices, input/output assets, and SMART/NEST devices) connected to the organization's network with the detailed information necessary for tracking and reporting. (NIST CF ID.AM-1; 2016 CIO FISMA Metrics 1.5, 3.17; NIST 800-53: CM-8) **Defined**

Met

2.1.2 Develops and maintains an up-to-date inventory of software platforms and applications used within the organization and with the detailed information necessary for tracking and reporting. (NIST 800-53: CM-8, NIST$_{CF\ ID.AM-2}$) **Defined**

Not Met

Comments:

OPM currently has several initiatives underway to improve its ardware and software inventory management program. The agency has recently made progress developing a list of its servers and databases, and uses an inventory management tool to track the software that is installed throughout the network.

However, lists of servers, databases, and software are only partial elements of a complete system inventory. OPM still has significant work ahead in converting the raw data it has collected into a comprehensive and mature system inventory. The current inventory data lists the devices and software that reside within the environment, but it does not describe which specific servers the software resides on, nor which information systems the devices and software support. The various elements of an inventory must be mapped to each other so that OPM can accurately define the boundaries of its information systems. A mature system inventory would not only identify all major information systems, but it would also contain details of the specific applications, software, servers, databases, and network devices that comprise and/or support each system. Furthermore, we issued a separate audit report on web application security that contained a recommendation related to OPM's lack of an adequate web application inventory.

2.1.3 Implements baseline configurations for IT systems that are developed and maintained in accordance with documented procedures. (NIST SP 800-53: CM-2; NIST$_{CF\ PR\ .IP-1}$) **Consistently s Implementeds**

Not Met

Section 2: Protect

Comments:

Our FY 2015 FISMA audit concluded that OPM did not have adequate configuration standards in place for all operating platforms that it uses. In FY 2016, OPM developed an inventory of servers, databases, and applications - a critical first step toward developing security configurations standards. The agency has also begun using configuration checklists from recognized industry organizations to help develop the agency's standard security configuration settings. However, we have not seen evidence that these standards have been developed and implemented for all operating systems identified in the inventory.

In addition to not having documented configuration standards for some systems, OPM has not documented its deviations from generic standards for all operating systems in the environment. OPM requires all configuration deviations to be reviewed through the change control process. However, once they are approved, these settings must be documented in the appropriate standard.

2.1.4 Implements and maintains standard security settings (also referred to as security configuration checklists or hardening guides) for IT systems in accordance with documented procedures. (NIST SP 800-53: CM-6; CIO 2016 FISMA Metrics, 2.3)

Consistently s Implementeds

Not Met

Comments: s

As stated in 2.1.3 above, we have not seen evidence that configuration standards have been developed and implemented for all operating systems identified in the inventory.

2.1.5 Assesses configuration change control processes, including processes to manage configuration deviations across the enterprise that are implemented and maintained. (NIST SP 800-53: CM-3, NIST CF PR.IP-3)

Managed and Measureable

Met

2.1.6 Identifies and documents deviations from configuration settings. Acceptable deviations are approved with business justification and risk acceptance. Where appropriate, automated means that enforce and redeploy configuration settings to systems at regularly scheduled intervals are deployed, while evidence of deviations is also maintained. (NIST SP 800-53: CM-6, Center for Internet Security Controls (CIS) 3.7)

Managed and Measureable

Not Met

Comments: s

As stated in 2.1.3 above, OPM has not documented its deviations from generic standards for all operating systems in the environment.

2.1.7 Implemented SCAP certified software assessing (scanning) capabilities against all systems on the network to assess both code-based and configuration-based vulnerabilities in accordance with risk management decisions. (NIST SP 800-53: RA-5, SI- 2; CIO 2016 FISMA Metrics 2.2, CIS 4.1)

Managed and Measureable

Section 2: Protect

Not Mets

Comments:

OPM performs automated network vulnerability scans on its systems on a bi-weekly basis. The recent improvements to the agency's system inventory provide some level of confidence that the vulnerability scans are actually hitting all systems within the environment.

While we acknowledge that improvements have been made to OPM's vulnerability scanning program, our test work performed during this audit indicates that several problems still exist. Specifically, the scanning tool did not have access to certain portions of OPM's internal network. In some cases, OPM was not aware of these access issues until they were identified by our test work. In addition, the historical scan reports that we reviewed indicate that most of the vulnerability scans performed in the first half of the fiscal year were not run with the system credentials necessary to perform a thorough analysis. However, OPM has recently made improvements to its scanning procedures to ensure that the scanning tools contain the necessary system credentials.

We also performed our own independent vulnerability scans on a sample of OPM's information systems. The results of our vulnerability scans indicate that OPM's production environment contains severely out-of-date and unsupported software and operating platforms. In other words, the software vendor no longer provides patches, security fixes, or updates for the software.

2.1.8 Remediates configuration-related vulnerabilities, including scan findings, in a timely manner as specified in organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)

Consistently s Implementeds

Not Met

Comments:

OPM distributes vulnerability scan results to the agency's 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, for other routine security weaknesses identified during vulnerability scans, OPM does not have a process to record or track the remediation status.

2.1.9 Develops and implements a patch management process in accordance with organization policy or standards, including timely and secure installation of software patches. (NIST SP 800-53: CM-3, SI-2, OMB M-16-04, DHS Binding Operational Directive 15-01)

Managed and Measureable

Not Met

Section 2: Protect

Comments:

OPM has a process in place for testing and installing patches for each operating system used within OPM's network. The OCIO has been transitioning some of the patching process to a new management utility, but not all systems and applications are integrated at this time. The servers that have not been integrated with this new utility are patched via other utilities or manual processes.

We made various efforts to validate the effectiveness of the OCIO's patch management process – both by performing our own independent vulnerability scans and by reviewing the results of historical vulnerability scans run by OPM. However, these efforts did not produce any evidence indicating that OPM's systems are consistently patched in a timely manner. Although we acknowledge that OPM is dedicating resources to improving its patch management process, we cannot at this time attest to any significant improvements in OPM's patch management process and therefore, our previous recommendation on this issue will be rolled forward in this report.

2.1.10 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. Based on all testing performed, is the Configuration Management Program effective?

Not Effective

Comments:

Based on the volume and criticality of metrics in this section that were not met, we do not believe that OPM's configuration management program is fully effective. However, we are optimistic that the agency appears to be taking steps to address the identified deficiencies.

Identity and Access Management (Protect)

2.2 Has the organization established an identity and access management program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**

Met

2.2.1 Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements, participate in required training prior to being granted access, and recertify access agreements on a predetermined interval. (NIST 800-53: PL-4, PS-6) **Consistently Implemented**

Met

2.2.2 Ensures that all users are only granted access based on least privilege and separation-of-duties principles. **Consistently Implemented**

Met

Section 2: Protect

2.2.3	Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. networking devices, such as load balancers and intrusion detection/prevention systems, and other input/output devices such as faxes and IP phones). **Met**	**Consistently Implemented**
2.2.4	Implements PIV for physical access in accordance with government policies. (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11) **Met**	**Consistently Implemented**
2.2.5	Implements PIV or a NIST Level of Assurance (LOA) 4 credential for logical access by all privileged users (system, network, database administrators, and others responsible for system/application control, monitoring, or administration functions). (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.5.1) **Met**	**Consistently Implemented**
2.2.6	Enforces PIV or a NIST LOA 4 credential for logical access for at least 85% of non-privileged users. (Cybersecurity Sprint, OMB M-16-04, PMC, 2016 CIO FISMA Metrics 2.4.1) **Met**	**Consistently Implemented**

Comments:

OPM-issued workstations can only be connected to the OPM network via two-factor authentication using PIV cards. In early FY 2016, OPM implemented controls that prevent non-OPM issued devices from connecting to the network. These controls close a previous loophole that allowed users to gain access to the network without PIV authentication. As such, OPM has successfully implemented a methodology that requires all users to connect to the network using PIV authentication. Although OPM has made progress in requiring PIV authentication to gain access to the network, this does not fully satisfy OMB mandates related to two-factor authentication. OMB Memorandum M-11-11 states that PIV credentials must be used to gain authorized access to an agency's 1) facilities, 2) network, and 3) information systems. OPM is not fully PIV compliant until all of its information systems (applications) can be accessed only via PIV authentication in lieu of a username and password. Our audit work indicated that only 2 of OPM's 46 major applications enforced PIV authentication.

2.2.7	Tracks and controls the use of administrative privileges and ensures that these privileges are periodically reviewed and R adjusted in accordance with organizationally defined timeframes. (2016 CIO FISMA Metrics 2.9, 2.10; OMB M-16-04, R CIS 5.2)R **Met**	**Managed and s Measureables**
2.2.8	Ensures that accounts are terminated or deactivated once access is no longer required or after a period of inactivity, according to organizational policy.	**Managed and Measureable**

Section 2: Protect

Not Mets

Comments: OPM has established a centralized process for securely granting employees and contractors access to its internal network. Our evaluation of OPM's termination process indicates that the process appears to work as intended for removing terminated agency (non-contractor) employees in a timely manner. However, the process for terminating access for contractor employees leaving the agency is not centrally managed, and it is the responsibility of the various Contractor 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.

2.2.9 Identifies, limits, and controls the use of shared accounts. (NIST SP 800-53: AC-2) — **Consistently Implemented**

Met

2.2.10 All users are uniquely identified and authenticated for remote access using Strong Authentication (multi-factor), including PIV. (NIST SP 800-46, Section 4.2, Section 5.1, NIST SP 800-63) — **Consistently Implemented**

Met

2.2.11 Protects against and detects unauthorized remote access connections or subversion of authorized remote access connections, including through remote scanning of host devices. (CIS 12.7, 12.8, FY 2016 CIO FISMA metrics 2.17.3, 2.17.4, 3.11, 3.11.1) — **Consistently Implemented**

Met

2.2.12 Remote access sessions are timed-out after 30 minutes of inactivity, requiring user re-authentication, consistent with OMB M-07-16 — **Managed and Measureable**

Not Met

Comments: Remote access sessions to OPM's network do not time out after 30 minutes of inactivity. OPM has conducted a risk assessment and has formally documented its acceptance of the associated risk.

2.2.13 Enforces a limit of consecutive invalid remote access logon attempts and automatically locks the account or delays the next logon prompt. (NIST 800-53: AC-7) — **Consistently Implemented**

Met

2.2.14 Implements a risk-based approach to ensure that all agency public websites and services are accessible through a secure connection through the use and enforcement of https and strict transport security. (OMB M-15-13) — **Consistently Implemented**

Not Met

Section 2: Protect

Comments:

In FY 2016, we evaluated OPM's efforts to implement Hyper Text Transport Protocol Secure (HTTPS) on all of its publicly accessible websites, as required by the OMB's memorandum M-15-13. Our results indicated that only a small percentage of OPM's publicly accessible websites were fully compliant with the regulation. In recent months OPM has made a significant effort to get all of its public websites compliant. OPM has stated that it currently has 47 of the 60 websites compliant, but the OIG has not performed additional independent testing after we issued the original results memorandum. We will continue to monitor OPM's progress with implementing the requirements outlined in OMB memorandum M-15-13 and will perform additional tests once OPM believes that it is 100 percent compliant.

2.2.15 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. Based on all testing performed is the Identity and Access Management Program effective?

Not Effective

Comments:

Based on the volume and criticality of metrics in this section that were not met, we do not believe that OPM's identity and access management program is fully effective. We believe that enforcing PIV authentication at the application level is a critical requirement for an effective program.

Security and Privacy T aining (Protect)

2.3 Has the organization established a security and privacy awareness and training program, including comprehensive agency policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**

Met

2.3.1 Develops training material for security and privacy awareness training containing appropriate content for the organization, including anti-phishing, malware defense, social engineering, and insider threat topics. (NIST SP 800-50, 800-53: AR-5, OMB M-15-01, 2016 CIO Metrics, PMC, National Insider Threat Policy (NITP)) **Consistently Implemented**

Met

2.3.2 Evaluates the skills of individuals with significant security and privacy responsibilities and provides additional security and privacy training content or implements human capital strategies to close identified gaps. (NIST SP 800-50) **Consistently Implemented**

Not Met

Comments:

While all employees completed the annual OPM security awareness training, only 73 percent of employees identified as having significant security responsibilities completed specialized IT training in FY 2016.

Section 2: Protect

2.3.3 Identifies and tracks status of security and privacy awareness training for all information system users (including employees, contractors, and other organization users) requiring security awareness training with appropriate internal processes to detect and correct deficiencies. (NIST 800-53: AT-2)

Consistently Implemented

Met

2.3.4 Identifies and tracks status of specialized security and privacy training for all personnel (including employees, contractors, and other organization users) with significant information security and privacy responsibilities requiring specialized training.

Consistently Implemented

Met

2.3.5 Measures the effectiveness of its security and privacy awareness and training programs, including through social engineering and phishing exercises. (PMC, 2016 CIO FISMA Metrics 2.19, NIST SP 800-50, NIST SP 800-55)

Managed and Measureable

Met

2.3.6 Provide any additional information on the effectiveness (positive or negative) of the organization's Security and Privacy Training Program that was not noted in the questions above. Based on all testing performed is the Security and Privacy Training Program effective?

Not Effective

Comments: Based on the criticality of the metric in this section that was not met, we do not believe that OPM's security and privacy training program is fully effective.

Level	Score	Possible Score
LEVEL 2: Defined	7	20

Section 3: Detect

Level 1

Definition

3.1.1 ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP800-137, OMB M-14-03, and the CIO ISCM CONOPS.

People

3.1.1.1 ISCM stakeholders and their responsibilities have not been fully defined and communicated across the organization. **Ad Hoc**

Met

3.1.1.2 The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. Key personnel do not possess knowledge, skills, and abilities to successfully implement an effective ISCM program. **Ad Hoc**

Met

3.1.1.3 The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk based decisions. **Ad Hoc**

Met

3.1.1.4 The organization has not defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. **Ad Hoc**

Met

Processes

3.1.1.5 ISCM processes have not been fully defined and are performed inan ad-hoc, reactive manner for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. **Ad Hoc**

Met

3.1.1.6 ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **Ad Hoc**

Met

3.1.1.7 The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. **Ad Hoc**

Section 3: Detect

Met

3.1.1.8 The organization has not defined its processes for collecting and considering lessons learned to improve ISCM processes. **Ad Hoc**

Met

Technology

3.1.1.9 The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. Use of ISCM technologies in the following areas is ad-hoc. **Ad Hoc**

- Patch management
- License management
- Information management
- Software assurance
- Vulnerability management
- Event management
- Malware detection
- Asset management
- Configuration management
- Network management
- Incident management

Met

3.1.1.10 The organization has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Ad Hoc**

Met

Level 2

Definition

3.2.1 The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide.

People

3.2.1.1 ISCM stakeholders and their responsibilities have been defined and communicated across the organization. However, stakeholders **Defined**

Section 3: Detect

may not have adequate resources (people, processes, and technology) to effectively implement ISCM activities.

Met

3.2.1.2 The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an ISCM program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective ISCM program. **Defined**

Met

3.2.1.3 The organization has defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. However, ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions. **Defined**

Met

3.2.1.4 The organization has defined how it will integrate ISCM activities with organizational risk tolerance, the threat environment, and business/mission requirements. However, ISCM activities are not consistently integrated with the organization's risk management program. **Defined**

Met

Processes

3.2.1.5 ISCM processes have been fully defined for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program. However, these processes are inconsistently implemented across the organization. **Defined**

Met

3.2.1.6 ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. **Defined**

Met

3.2.1.7 The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. **Defined**

Met

3.2.1.8 The organization has a defined process for capturing lessons learned on the effectiveness of its ISCM program and making necessary improvements. However, lessons learned are not consistently shared across the organization and used to make timely improvements **Defined**

Section 3: Detect

to the ISCM program.

Met

Technology

3.2.1.9 The organization has identified and fully defined the ISCM technologies it plans to utilize in the following automation areas. In addition, the organization has developed a plan for implementing ISCM technologies in these areas: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. However, the organization has not fully implemented technology is these automation areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while automated tools are implemented to support some ISCM activities, the tools may not be interoperable. **Defined**

Met

3.2.1.10 The organization has defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. However, the organization does not consistently implement the technologies that will enable it to manage an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Defined**

Met

Level 3

Definition

3.3.1 In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions, consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.

People

3.3.1.1 ISCM stakeholders and their responsibilities have been identified and communicated across the organization, and stakeholders have adequate resources (people, processes, and technology) to effectively implement ISCM activities. **Consistently Implemented**

Not Met

Section 3: Detect

Comments:

There has been an extremely high employee turnover rate for OPM's critical "Information System Security Officer" positions, and the agency has struggled to backfill these vacancies. In addition, there have been five different individuals in the role of the Chief Information Officer in the past three years. The negative impact of these staffing issues is apparent in the results of our current FISMA audit work. There has been a significant regression in OPM's compliance with FISMA requirements including continuous monitoring, as the agency failed to meet requirements that it had successfully met in prior years. Therefore, we do not believe OPM has adequate resources (people, processes, and technology) currently in place to effectively implement ISCM activities.

3.3.1.2 The organization has fully implemented its plans to close any gapes in skills, knowledge, and resources required to successfully implement an ISCM program. Personnel possess the required knowledge, skills, and abilities to effectively implement the organization's ISCM program.

Consistently s Implementeds

Not Met

Comments:

As mentioned in section 3.3.1.2 above, there has been extremely high employee turnover at critical information security positions. Although there has been a recent surge in hiring individuals for this position, simply having the staff on board does not guarantee that the team can effectively manage information security and keep OPM compliant with FISMA requirements. The agency must continue its efforts to close gaps in skills and knowledge of these individuals.

3.3.1.3 ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations.

Consistently Implemented

Not Met

Comments:

OPM has not fully implemented an effective process for continuously monitoring security controls. Therefore the agency is not yet able to provide key officials with results of ISCM processes to make risk based decisions.

3.3.1.4 ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements.

Consistently Implemented

Not Met

Comments:

OPM has not fully implemented an effective process for continuously monitoring security controls. Therefore the agency is not yet able to fully integrate ISCM activity into its risk management program.

Processes

3.3.1.5 ISCM processes are consistently performed across the organization in the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing

Consistently Implemented

Section 3: Detect

ISCM data, reporting findings, and determining the appropriate risk responses; and reviewing and updating the ISCM program.

Met

3.3.1.6 The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. **Consistently Implemented**

Met

3.3.1.7 The organization is consistently capturing qualitative and quantitative performance measures on the performance of its ISCM program in accordance with established requirements for data collection, storage, analysis, retrieval, and reporting. ISCM measures provide information on the effectiveness of ISCM processes and activities. **Consistently Implemented**

Not Met

Comments: s OPM had previously established qualitative and quantitative measures to evaluate its continuous monitoring program - this was done by performing quarterly security control tests and feeding these results into an ISCM dashboard. However, these tests were not performed for a significant number of systems throughout FY 2016.

3.3.1.8 The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes. **Consistently Implemented**

Met

3.3.1.9 The organization has consistently implemented its defined technologies in all of the following ISCM automation areas. ISCM tools are interoperable to the extent practicable. **Consistently Implemented**

- Patch management
- License management
- Information management
- Software assurance
- Vulnerability management
- Event management
- Malware detection
- Asset management
- Configuration management
- Network management
- Incident management

Met

Section 3: Detect

Technology

3.3.1.10 The organization can produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network and the security configuration of these devices and software. **Consistently Implemented**

Met

Level 4

Definition

3.4.1 In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.

People

3.4.1.1 The organization's staff is consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of the organization's ISCM program. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 4 requirements.

3.4.1.2 Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the ISCM program. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 4 requirements.

3.4.1.3 Staff are assigned responsibilities for developing and monitoring ISCM metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the ISCM program. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 4 requirements.

Processes

Section 3: Detect

3.4.1.4 The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing ISCM. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 4 requirements.

3.4.1.5 Data supporting ISCM metrics are obtained accurately, consistently, and in a reproducible format. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 4 requirements.

3.4.1.6 The organization is able to integrate metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 4 requirements.

3.4.1.7 The organization uses its ISCM metrics for determining risk response actions including risk acceptance, avoidance/rejection, or transfer. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 4 requirements.

3.4.1.8 ISCM metrics are reported to the organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 4 requirements.

Section 3: Detect

3.4.1.9 ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 4 requirements.

Technology

3.4.1.10 The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing ISCM. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 4 requirements.

3.4.1.11 The organization's ISCM performance measures include data on the implementation of its ISCM program for all sections of the network from the implementation of technologies that provide standard calculations, comparisons, and presentations. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 4 requirements.

3.4.1.12 The organization utilizes a SIEM tool to collect, maintain, monitor, and analyze IT security information, achieve situational awareness, and manage risk **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 4 requirements.

Level 5

Definition

3.5.1 In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, R self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing R threat and technology landscape.R

Section 3: Detect

Peoples

3.5.1.1 The organization's assigned personnel collectively possess a high skill level to perform and update ISCM activities on a near real-time basis to make any changes needed to address ISCM results based on organization risk tolerance, the threat environment, and business/mission requirements. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 5 requirements.

Processes

3.5.1.2 The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity and practices. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 5 requirements.

3.5.1.3 On a near real-time basis, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 5 requirements.

3.5.1.4 The ISCM program is fully integrated with strategic planning, enterprise architecture and capital planning and investment control processes, and other mission/business areas, as appropriate. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 5 requirements.

3.5.1.5 The ISCM program achieves cost-effective IT$_{\text{security objectives}}$ and goals and influences decision making that is based on cost, risk, and mission impact. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 5 requirements.

Section 3: Detect

Technology

3.5.1.6 The organization has institutionalized the implementation of advanced cybersecurity technologies in near real-time. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 5 requirements.

3.5.1.7 The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its ISCM program. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the ISCM maturity model, and therefore is not able to implement level 5 requirements.

Level	Score	Possible Score
LEVEL 3: Consistently Implemented	13	20

Section 4: Respond

Level 1

Definition

4.1.1 Incident response program is not formalized and incident response activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines).

People

4.1.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have not been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. **Ad Hoc**

Met

4.1.1.2 The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. Key personnel do not possess the knowledge, skills, and abilities to successfully implement an effective incident response program. **Ad Hoc**

Met

4.1.1.3 The organization has not defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. **Ad Hoc**

Met

4.1.1.4 The organization has not defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Ad Hoc**

Met

Processes

4.1.1.5 Incident response processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting to internal and external stakeholders using standard data elements and impact classifications within timeframes established by US-CERT. **Ad Hoc**

Met

4.1.1.6 The organization has not fully defined how it will collaborate with DHS and other parties, as appropriate, to provide on-site, technical **Ad Hoc**

Section 4: Respond

assistance/surge resources/special capabilities for quickly responding to incidents.

Met

4.1.1.7 The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. **Ad Hoc**

Met

4.1.1.8 The organization has not defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. **Ad Hoc**

Met

Technology

4.1.1.9 The organization has not identified and defined the incident response technologies needed in one or more of the following areas and relies on manual/procedural methods in instances where automation would be more effective. Use of incident response technologies in the following areas is ad-hoc. **Ad Hoc**

- 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 anti-virus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools

Met

4.1.1.10 The organization has not defined how it will meet the defined Trusted Internet Connection (TIC) security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. **Ad Hoc**

Met

4.1.1.11 The organization has not defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving the organization's networks. **Ad Hoc**

Met

4.1.1.12 The organization has not defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. **Ad Hoc**

Met

Level 2

Section 4: Respond

Definition

4.2.1 The organizational has formalized its incident response programthrough the development of comprehensive incident response policies, plans, and procedures consistent with FISMA (including guidance from NIST SP 800-83, NISTSP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, incident response policies, plans, and procedures are not consistently implemented organization-wide.

People

4.2.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined and communicated across the organization, including the designation of a principal security operations center or equivalent organization that is accountable to agency leadership, DHS, and OMB for all incident response activities. However, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement incident response activities. Further, the organization has not verified roles and responsibilities as part of incident response testing. **Defined**

Met

4.2.1.2 The organization has performed an assessment of the skills, knowledge, and resources needed to effectively implement an incident response program. In addition, the organization has developed a plan for closing any gaps identified. However, key personnel may still lack the knowledge, skills, and abilities to successfully implement an effective incident response program. **Defined**

Met

4.2.1.3 The organization has defined a common threat vector taxonomy and defined how incident response information will be shared with individuals with significant security responsibilities and other stakeholders, and used to make timely, risk-based decisions. However, the organization does not consistently utilize its threat vector taxonomy and incident response information is not always shared with individuals with significant security responsibilities and other stakeholders in a timely manner. **Defined**

Met

4.2.1.4 The organization has defined how it will integrate incident response activities with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. However, incident response activities are not consistently integrated with these areas. **Defined**

Met

Processes

4.2.1.5 Incident response processes have been fully defined for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, **Defined**

Section 4: Respond

and reporting using standard data elements and impact classifications within timeframes established by US-CERT. However, these processes are inconsistently implemented across the organization.

Met

4.2.1.6 The organization has fully defined, but not consistently implemented, its processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents. **Defined**

Met

4.2.1.7 The organization has identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its incident response program, perform trend analysis, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. **Defined**

Met

4.2.1.8 The organization has defined its processes for collecting and considering lessons learned and incident data to improve security controls and incident response processes. However, lessons learned are not consistently captured and shared across the organization and used to make timely improvements to security controls and the incident response program. **Defined**

Met

Technology

4.2.1.9 The organization has identified and fully defined the incident response technologies it plans to utilize in the following areas: **Defined**

- 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. However, the organization has not ensured that security and event data are aggregated and correlated from all relevant sources and sensors.
- Malware detection such as Anti-virus and antispam software technologies
- Information management such as data loss prevention
- File integrity and endpoint and server security tools

However, the organization has not fully implemented technologies in these areas and continues to rely on manual/procedural methods in instances where automation would be more effective. In addition, while tools are implemented to support some incident response activities, the tools are not interoperable to the extent practicable, do not cover all components of the organization's network, and/or have not been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, plans, and procedures.

Met

Section 4: Respond

4.2.1.10 The organization has defined how it will meet the defined TIC security controls and ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. However, the organization has not ensured that the TIC 2.0 provider and agency managed capabilities are consistently implemented. **Defined**

Met

4.2.1.11 The organization has defined how it plans to utilize DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving its networks. **Defined**

Met

4.2.1.12 The organization has defined how it plans to utilize technology to develop and maintain a baseline of network operations and expected data flows for users and systems. However, the organization has not established, and does not consistently maintain, a comprehensive baseline of network operations and expected data flows for users and systems. **Defined**

Met

Level 3

Definition

4.3.1 In addition to the formalization and definition of its incident response program (Level 2), the organization consistently implements its incident response program across the agency, in accordance with FISMA (including guidance from NIST SP 800-83, NIST SP 800-61 Rev. 2, NIST SP 800-53, OMB M-16-03, OMB M-16-04, and US-CERT Federal Incident Notification Guidelines). However, data supporting metrics on the effectiveness of the incident response program across the organization are not verified, analyzed, and correlated.

People

4.3.1.1 Incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies have been fully defined, communicated, and consistently implemented across the organization (Level 2). Further, the organization has verified roles and responsibilities of incident response stakeholders as part of incident response testing. **Consistently Implemented**

Met

4.3.1.2 The organization has fully implemented its plans to close any gaps in the skills, knowledge, and resources needed to effectively implement its incident response program. Incident response teams are periodically trained to ensure that knowledge, skills, and abilities are maintained. **Consistently Implemented**

Met

Section 4: Respond

4.3.1.3	The organization consistently utilizes its defined threat vector taxonomy and shares information with individuals with significant security responsibilities and other stakeholders in a timely fashion to support risk-based decision making. **Met**	**Consistently Implemented**
4.3.1.4	Incident response activities are integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Met**	**Consistently Implemented**

Processes

4.3.1.5	Incident response processes are consistently implemented across the organization for the following areas: incident response planning, incident response training and testing; incident detection and analysis; incident containment, eradication, and recovery; incident coordination, information sharing, and reporting using standard data elements and impact classifications within timeframes established by US-CERT. **Met**	**Consistently Implemented**
4.3.1.6	The organization has ensured that processes to collaborate with DHS and other parties as appropriate, to provide on-site, technical assistance/surge resources/special capabilities for quickly responding to incidents are implemented consistently across the organization. **Met**	**Consistently Implemented**
4.3.1.7	The organization is consistently capturing qualitative and quantitative performance metrics on the performance of its incident response program. However, the organization has not ensured that the data supporting the metrics was obtained accurately and in a reproducible format or that the data is analyzed and correlated in ways that are effective for risk management. **Met**	**Consistently Implemented**
4.3.1.8	The organization is consistently collecting and capturing lessons learned and incident data on the effectiveness of its incident response program and activities. However, lessons learned may not be shared across the organization in a timely manner and used to make timely improvements to the incident response program and security measures. **Met**	**Consistently Implemented**
4.3.1.9	The rigor, intensity, scope, and results of incident response activities (i.e. preparation, detection, analysis, containment, eradication, and recovery, reporting and post incident) are comparable and predictable across the organization. **Met**	**Consistently Implemented**

Technology

Section 4: Respond

4.3.1.10 The organization has consistently implemented its defined incident response technologies in the following areas: **Consistently s Implementeds**
- 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. The organization ensures that security and event data are aggregated and correlated from all relevant sources and sensors
- Malware detection, such as anti-virus and antispam software technologies
- Information management, such as data loss prevention
- File integrity and endpoint and server security tools

In addition, the tools are interoperable to the extent practicable, cover all components of the organization's network, and have been configured to collect and retain relevant and meaningful data consistent with the organization's incident response policy, procedures, and plans.

Met

4.3.1.11 The organization has consistently implemented defined TIC security controls and implemented actions to ensure that all agency traffic, including mobile and cloud, are routed through defined access points, as appropriate. **Consistently s Implementeds**

Not Met

Comments: s OPM has stated that it has implemented several TIC security controls across the organization, but it has not provided evidence supporting this statement.

4.3.1.12 The organization is utilizing DHS' Einstein program for intrusion detection/prevention capabilities for traffic entering and leaving their networks. **Consistently Implemented**

Met

4.3.1.13 The organization has fully implemented technologies to develop and maintain a baseline of network operations and expected data flows for users and systems. **Consistently Implemented**

Not Met

Comments: OPM currently uses various software tools to define the overall baseline activity of its network. However, the agency has not completed a baseline specific to users, and currently do not have any tools or software to monitor and alert on unusual user activity. OPM is currently in the process of acquiring a software product to address this issue.

Level 4

Definition

4.4.1 In addition to being consistently implemented (Level 3), incident response activities are repeatable and metrics are used to

Section 4: Respond

measure and manage the implementation of the incident response program, achieve situational awareness, and control ongoing risk. In addition, the incident response program adapts to new requirements and government-wide priorities.

People

4.4.1.1 Incident response stakeholders are consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and are collecting, analyzing, and reporting data on the effectiveness of the organization's incident response program. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 4 requirements.

4.4.1.2 Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the incident response program. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 4 requirements.

4.4.1.3 Incident response stakeholders are assigned responsibilities for developing and monitoring incident response metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the incident response program. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 4 requirements.

Processes

4.4.1.4 The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing incident response. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 4 requirements.

Section 4: Respond

4.4.1.5 Data supporting incident response measures and metrics are obtained accurately, consistently, and in a reproducible format. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 4 requirements.

4.4.1.6 Incident response data, measures, and metrics are analyzed, collected, and presented using standard calculations, comparisons, and presentations **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 4 requirements.

4.4.1.7 Incident response metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 4 requirements.

Technology

4.4.1.8 The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing incident response activities. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 4 requirements.

4.4.1.9 The organization's incident response performance measures include data on the implementation of its incident response program for all sections of the network. **Managed and Measureable**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 4 requirements.

Level 5

Section 4: Respond

Definition

4.5.1 In addition to being managed and measurable (Level 4), the organization's incident response program is institutionalized,R repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements, and R a changing threat and technology landscape.R

People

4.5.1.1 The organization's assigned personnel collectively possess a high skill level to perform and update incident response activities on a near real-time basis to make any changes needed to address incident response results based on organization risk tolerance, the threat environment, and business/mission requirements. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 5 requirements.

Processes

4.5.1.2 The organization has institutionalized a process of continuous improvement incorporating advanced cybersecurity practices. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 5 requirements.

4.5.1.3 On a near real-time basis, the organization actively adapts its incident response program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a near real-time manner. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 5 requirements.

4.5.1.4 The incident response program is fully integrated with organizational risk management, continuous monitoring, continuity of operations, and other mission/business areas, as appropriate. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 5 requirements.

4.5.1.5 The incident response program achieves cost-effective IT security objectives and goals and influences decision making that is based **Optimized**

Section 4: Respond

on cost, risk, and mission impact.

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 5 requirements.

Technology

4.5.1.6 The organization has institutionalized the implementation of advanced incident response technologies in near real-time. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 5 requirements.

4.5.1.7 The organization has institutionalized the use of advanced technologies for analysis of trends and performance against benchmarks to continuously improve its incident response program. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 5 requirements.

4.5.1.8 The organization uses simulation based technologies to continuously determine the impact of potential security incidents to its IT assets and adjusts incident response processes and security measures accordingly. **Optimized**

Not Met

Comments: OPM has not implemented all the requirements for level 3 (Consistently Implemented) of the incident response maturity model, and therefore is not able to implement level 5 requirements.

Level	Score	Possible Score
LEVEL 3: Consistently Implemented	13	20

Section 5: Recover

Contingency Planning (Recover)

5.1 Has the organization established an enterprise-wide business continuity/disaster recovery program, including policies and procedures consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? **Defined**

Met

5.1.1 Develops and facilitates recovery testing, training, and exercise (TT&E) programs. (FCD1, NIST SP 800-34, NIST SP 800-53) **Consistently Implemented**

Not Met

Comments: Contingency plans exist for 45 out of 46 OPM major systems. However, only 17 of the plans have been reviewed within the current fiscal year. Therefore, we do not believe that these documents have been adequately maintained and updated to address that the ongoing changes to OPM's infrastructure. In addition, only 2 of the 45 contingency plans were subject to an adequate test in FY 2016. Furthermore, 9 of the contingency plans have not been tested at all since 2014.

5.1.2 Incorporates the system's Business Impact Analysis and Business Process Analysis into analysis and strategy toward development of the organization's Continuity of Operations Plan, Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP). (NIST SP 800-34) **Consistently Implemented**

Met

5.1.3 Develops and maintains documented recovery strategies, plans, and procedures at the division, component, and IT infrastructure levels. (NIST SP 800-34) **Consistently Implemented**

Not Met

Comments: As stated in 5.1.1 above, many of OPM's contingency plans are not maintained and remain out-of-date.

5.1.4 BCP and DRP are in place and ready to be executed upon if necessary. (FCD1, NIST SP 800-34, 2016 CIO FISMA Metrics 5.3, PMC) **Consistently Implemented**

Met

5.1.5 Tests BCP and DRP for effectiveness and updates plans as necessary. (2016 CIO FISMA Metrics, 5.4) **Managed and Measureable**

Not Met

Section 5: Recover

Comments: We received contingency plans for 45 out of 46 OPM major systems. However, only 17 of the plans received had been reviewed within the current fiscal year. Therefore, we do not believe that these documents have been adequately maintained and updated to address the ongoing changes to OPM's infrastructure. Maintaining an up-to-date contingency plan is a critical element to ensuring information systems can be properly recovered in the event of an emergency or disaster. OPM's Information Security Privacy and Policy Handbook obligates system owners to test or exercise each system's contingency plans at least annually. During the course of our audit we received evidence that only two of OPM's 46 major information systems was subject to an adequate contingency plan test in FY 2016. Furthermore, 9 of the 46 major systems have not been tested at all since 2014.

5.1.6 Tests system-specific contingency plans, in accordance with organizationally defined timeframes, to determine the effectiveness of the plans as well as readiness to execute the plans if necessary. (NIST SP 800-53: CP-4) **Consistently s Implementeds**

Not Met

Comments: As stated in 5.1.1 above, many of OPM's contingency plans were not tested this fiscal year.

5.1.7 Develops after-action reports that address issues identified during contingency/disaster recovery exercises in order to improve contingency/disaster recovery processes. (FCD1, NIST SP 800-34) **Managed and Measureable**

Not Met

Comments: As stated in 5.1.1 above, many of OPM's contingency plans were not tested this fiscal year, therefore it was not possible to perform after-action reports.

5.1.8 Determines alternate processing and storage sites based upon risk assessments which ensure the potential disruption of the organization's ability to initiate and sustain operations is minimized, and are not subject to the same physical and/or cybersecurity risks as the primary sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-6, CP-7) **Consistently Implemented**

Not Met

Comments: OPM policy requires risk assessments to be incorporated into its contingency plans. However, as stated in 5.1.1 above, very few of OMP's contingency plans have been reviewed in the past year and therefore we cannot express confidence that these risk assessments are based on current and relevant information.

5.1.9 Conducts backups of information at the user- and system-levels and protects the confidentiality, integrity, and availability of backup information at storage sites. (FCD1, NIST SP 800-34, NIST SP 800-53: CP-9, NIST CF, PR.IP-4, NARA guidance on information systems security records) **Managed and Measureable**

Met

Section 5: Recover

5.1.10 Contingency planning that considers supply chain threats. **Defined**

Not Met

Comments: The contingency plan for OPM's general support system states that supply chain threats have been identified and certain individuals are responsible for identifying lead times and necessary equipment replacements. However, we have not received evidence to support this statement.

5.1.11 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. Based on all testing performed is the Contingency Planning Program effective?

Not Effective

Comments: Based on the volume and criticality of metrics in this section that were not met, we do not believe that OPM's contingency planning program is fully effective.

Level	Score	Possible Score
LEVEL 2: Defined	7	20

APPENDIX A: Maturity Model Scoring

Maturity Levels by Section

Section	Level	Score	Possible Score
Section 1: Identify	LEVEL2: Defined	7	20
Section 2: Protect	LEVEL2: Defined	7	20
Section 3: Detect	LEVEL3: Consistently Implemented	13	20
Section 4: Respond	LEVEL3: Consistently Implemented	13	20
Section 5: Recover	LEVEL2: Defined	7	20
TOTAL		47	100

Section 1: Identifys

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	2	2	4	50%	4	4
Consistently Implemented	6	5	11	55%	0	6
Managed and Measureable	2	4	6	33%	0	5
Optimized	0	0	0	100%	0	2

Section 2: Protects

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	4	1	5	80%	4	4
Consistently Implemented	13	5	18	72%	0	6
Managed and Measureable	3	5	8	38%	0	5
Optimized	0	0	0	100%	0	2

Section 3: Detects

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	10	0	10	100%	3	3
Defined	10	0	10	100%	4	4
Consistently Implemented	5	5	10	50%	6	6
Managed and Measureable	0	12	12	0%	0	5
Optimized	0	7	7	0%	0	2

Section 4: Respond

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	12	0	12	100%	3	3
Defined	12	0	12	100%	4	4
Consistently Implemented	11	2	13	85%	6	6
Managed and Measureable	0	9	9	0%	0	5
Optimized	0	8	8	0%	0	2

Section 5: Recovers

Model Indicator	Met	Not Met	Total	%	Points Assigned	Possible Points
Ad-Hoc	0	0	0	100%	3	3
Defined	1	1	2	50%	4	4
Consistently Implemented	2	4	6	33%	0	6
Managed and Measureable	1	2	3	33%	0	5
Optimized	0	0	0	100%	0	2

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

-- CAUTION --