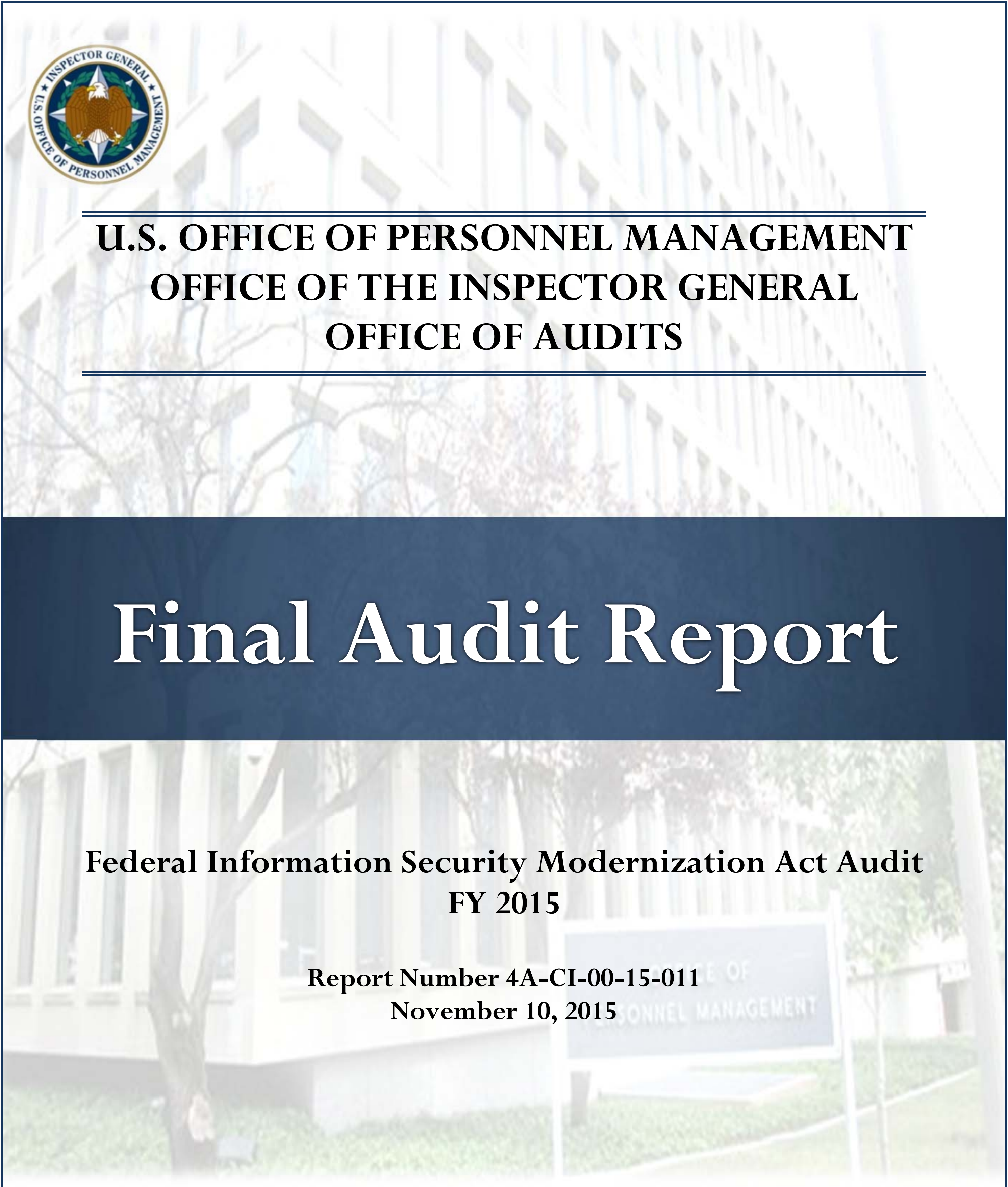

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Federal Information Security Modernization Act Audit
FY 2015

Report Number 4A-CI-00-15-011
November 10, 2015

-- CAUTION --

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage (*http://www.opm.gov/our-inspector-general*), caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

EXECUTIVE SUMMARY

Federal Information Security Modernization Act Audit – FY 2015

Report No. 4A-CI-00-15-011 **November 10, 2015**

Why Did We Conduct the Audit?

Our overall objective was to evaluate OPM's 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 Department of Homeland Security's (DHS) FISMA Inspector General reporting instructions.

What Did We Audit?

The Office of the Inspector General (OIG) 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 2015 at OPM headquarters in Washington, D.C.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

In FY 2015 OPM was the victim of a massive data breach that involved the theft of sensitive personal information of millions of individuals. For many years we have reported critical weaknesses in OPM's ability to manage its information technology (IT) environment, and warned that the agency was at an increased risk of a data breach. In the wake of this data breach, OPM is finally focusing its efforts on improving its IT security posture. Unfortunately, as indicated by the variety of findings in this audit report, OPM continues to struggle to meet many FISMA requirements.

During this audit we did close a long-standing recommendation related to OPM's information security management structure. However, this audit also determined that there has been a regression in OPM's management of its system Authorization program, which we classified as a material weakness in the FY 2014 FISMA audit report. 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. Should this moratorium on Authorizations continue, the agency will have up to 23 systems that have not been subject to a thorough security controls assessment.

We continue to believe that OPM's management of system Authorizations represents a material weakness in the internal control structure of the agency's IT security program. The moratorium on Authorizations will result in the IT security controls of OPM's systems being neglected. Combined with the inadequacy and non-compliance of OPM's continuous monitoring program, we are very concerned that the agency's systems will not be protected against another attack.

Additionally, OPM's inability to accurately inventory its systems and network devices drastically diminishes the effectiveness of its security controls. OPM has implemented a large number of improved security monitoring tools, but without a complete understanding of its network, it cannot adequately monitor its environment and therefore the usefulness of these tools is reduced.

The following page outlines the additional issues that we identified during this FY 2015 FISMA audit.

EXECUTIVE SUMMARY

Federal Information Security Modernization Act Audit – FY 2015

Summary of FY 2015 FISMA Results

- The significant deficiency related to information security governance has been dropped due to the reorganization of the Office of the Chief Information Officer (OCIO).
- OPM's system development life cycle policy is not enforced for all system development projects.
- OPM does not maintain a comprehensive inventory of servers, databases, and network devices.
- Up to 23 major OPM information systems are operating without a valid Authorization. This represents a material weakness in the internal control structure of OPM's IT security program.
- OPM does not have a mature continuous monitoring program. Also, security controls for all OPM systems are not adequately tested in accordance with OPM policy.
- The OCIO has implemented an agency-wide information system configuration management policy; however, configuration baselines have not been created for all operating platforms. Also, all operating platforms are not routinely scanned for compliance with configuration baselines.
- We are unable to independently attest that OPM has a mature vulnerability scanning program.
- Multi-factor authentication is not required to access OPM systems in accordance with OMB memorandum M-11-11.
- OPM has established an Enterprise Network Security Operations Center that is responsible for incident detection and response.
- 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.
- Program offices are not adequately incorporating known weaknesses into Plans of Action and Milestones (POA&M) and the majority of systems contain POA&Ms that are over 120 days overdue.
- OPM has not configured its virtual private network servers to automatically terminate remote sessions in accordance with agency policy.
- Not all OPM systems have reviewed their contingency plans or conducted contingency plan tests in FY 2015.
- Several information security agreements between OPM and contractor-operated information systems have expired.

ABBREVIATIONS

Authorization	Security Assessment and Authorization
CDM	Continuous Diagnostic and Mitigation
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
DSO	Designated Security Officer
ENSOC	Enterprise Network Security Operations Center
FIPS	Federal Information Processing Standards
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
LAN	Local area network
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	Office of Management and Budget
OPM	Office of Personnel Management
POA&M	Plan of Action and Milestones
SDLC	System Development Life Cycle
SIEM	Security information and event management
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual private network

TABLE OF CONTENTS

Page

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 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 evaluation of OPM's security program and practices. As part of our evaluation, 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 reemphasizes 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) 2015 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. OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

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:

- Continuous Monitoring Management;
- Configuration Management;
- Identity and Access Management;
- Incident Response and Reporting;
- Risk Management;
- Security Training;
- Plan of Action & Milestones (POA&M);
- Remote Access Management;
- Contingency Planning; and
- Contractor Systems.

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 audited the security controls of four major applications/systems at OPM (see the Scope and Methodology section below for details of these audits), and followed-up on outstanding recommendations from prior FISMA audits (see Appendix I).

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 2015.

We reviewed OPM's general FISMA compliance efforts in the specific areas defined in DHS's guidance and the corresponding reporting instructions. We also performed information security audits on the following major information systems:

- Multi-State Plan Program Portal (Report No. 4A-RI-00-15-013, issued May 11, 2015);
- USA Performance System (Report No. 4A-HR-00-15-018, issued July 20, 2015);

- Annuitant Health Benefits Open Season System (Report No. 4A-RI-00-15-019, issued July 29, 2015); and,
- GP Plateau Baseline 6 Learning Management System (Report No. 4A-HR-00-15-015, issued July 31, 2015).

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 2015 Inspector General Federal Information Security Modernization Act Reporting Instructions;
- OPM Information Technology Security and Privacy Policy Handbook;
- OPM Information Technology Security FISMA Procedures;
- OPM Security Assessment and Authorization Guide;
- OPM Plan of Action and Milestones Standard Operating Procedures;
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive 12;
- P.L. 107-347, Title III, Federal Information Security Management Act of 2002;

- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- National Institute for Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security;
- 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 2015 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 RECOMMEDATIONS

Introduction

In FY 2015 OPM was the victim of a massive data breach that involved the theft of sensitive personal information of millions of individuals. This was an advanced attack that may have been impossible to prevent in even the most advanced network environment. However, for many years we have reported critical weaknesses in OPM's ability to manage its IT environment, and warned that the agency was at an increased risk of a data breach. OPM continuously failed a variety of FISMA metrics and carried material weaknesses in the annual FISMA reports. Our recommendations appeared to garner little attention, as the same findings were repeated year after year.

In the wake of this data breach, OPM is finally focusing its efforts on improving its IT security posture. Unfortunately, as indicated by the variety of findings in this audit report, OPM continues to fail to meet FISMA requirements, and we now have additional concerns with the manner in which the agency is attempting to quickly fix problems that were decades in the making.

OPM has determined that in order to best secure the sensitive data it maintains, it must create an entirely new technical infrastructure and migrate all of the agency's systems into this new environment (referred to as the 'Shell'). OPM faces enormous hurdles in reaching its desired outcome – many of which we do not believe the agency is adequately prepared to address. This infrastructure improvement project has an impact on a variety of the FY 2015 FISMA reporting metrics and will be referenced throughout this report. However, our specific concerns with this project are detailed through separate reporting mechanisms. [1]

Of particular concern in this year's FISMA audit results is the overall lack of compliance that seems to permeate the agency's IT security program. For example, OPM's decision to put system Security Assessment and Authorizations on hold until applications are migrated into the Shell is an extremely poor decision, and makes it likely that the IT security controls of OPM's systems will remain neglected during the time that it takes to move the systems to the new environment (probably many years – see section B below). Combined with the inadequacy and non-compliance of OPM's continuous monitoring program, we are very concerned that the agency's systems will not be protected against another attack.

[1] Flash Audit Alert – U.S. Office of Personnel Management's Infrastructure Improvement Project (Report No. 4A-CI-00-15-055) and Interim Status Report on OPM's Responses to Flash Audit Alert – U.S. Office of Personnel Management's (OPM) Infrastructure Improvement Project (Report No. 4A-CI-00-15-055)

Additionally, OPM's inability to accurately inventory its systems and network devices drastically diminishes the effectiveness of its security controls. OPM has implemented a large number of improved security monitoring tools, but without a complete understanding of its network, it cannot adequately monitor its environment and therefore the usefulness of these tools is reduced. This same concern extends to OPM's vulnerability scanning program (see section D below).

In its response to our draft audit report, the OPM Office of the Chief Information Officer (OCIO) stated "*I am proud that OCIO has closed 77% of the recommendations for the FY 2007 through FY 2014 OIG FISMA Audits, as well as OIG system audits.*" Although this number is technically accurate, the vast majority of those recommendations were closed many years ago, and are no longer relevant to the current cybersecurity threats that the agency faces. A more relevant statistic is that OPM has closed only 43% of the FISMA recommendations issued in the FY 2013 and FY 2014 FISMA audits. In addition, 21 of the 27 recommendations in this FY 2015 report are at least one year old[2].

21 of the 27 recommendations in this report are at least one year old.

We acknowledge that OPM has recently placed additional focus on addressing OIG audit recommendations, and has sought our input in implementing controls to protect its technical environment. Significant work remains for the agency to secure its IT systems, and we are hopeful that this trend continues through the next fiscal year.

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 involves a variety of activities, challenges, and requirements, but three primary elements include a well-defined security management structure, maintaining a comprehensive inventory of information systems, and managing systems development projects in a disciplined and consistent manner.

The following sections provide additional details from the OIG's review of IT security governance at OPM.

a) Security Management Structure

For many years, we have reported increasing concerns about the state of OPM's information security management structure. Our Federal Information Security Management Act 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

[2] Two of the 27 recommendations in this report were implemented by the OCIO in early FY 2016, including one recommendation that was more than one year old, and will be closed upon issuance of this report.

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 imminently hire enough ISSOs to manage the security for 100 percent of the agency's information systems. Throughout FY 2015, OPM was successful in filling the vacant ISSO positions, effectively centralizing IT security responsibility under the Chief Information Officer (CIO) and fulfilling our audit recommendation.

OPM has made progress in addressing security governance issues by centralizing IT security responsibility.

With this new governance structure in place, we are closing the audit recommendation related to security management structure and removing the significant deficiency from our report. However, the reorganization of IT security responsibility is only the first step in addressing OPM's security governance issues. We will closely monitor the effectiveness of this new management structure and will issue additional audit recommendations as necessary.

b) Infrastructure and Inventory

In addition to the decentralization of personnel with IT responsibility, OPM has historically maintained a fragmented and decentralized technical infrastructure that is spread over six data centers and is maintained by different organizations within the agency. OPM's various program offices would procure, configure, and manage their own information systems, and the OCIO had little control over them – assuming it knew they existed.

OPM has several initiatives underway to improve its inventory management program, but it is a monumental task. During this audit we reviewed OPM's inventory of major information systems (i.e., those subject to FISMA reporting requirements) and compared it to a "comprehensive inventory" that was developed in preparation for migrating systems to the new Shell environment. There are significant discrepancies between the two lists, and our primary concern is that there are still unidentified systems residing on OPM's network, and that existing applications are not appropriately classified as major or minor.

Over the past several years, the agency has procured a variety of tools to help automate efforts to secure the OPM network. However, our FY 2014 FISMA audit determined that all of these tools are not being utilized to their fullest capacity, as the agency was having difficulty implementing and enforcing the new controls on all endpoints of the decentralized network. In the wake of the data breach, OPM procured even more security tools to help further secure the network. We agree that these tools add value, but OPM continues to face the challenge of implementing them into a fragmented environment where it continues to lack a comprehensive inventory of information systems, computer hardware, and network devices. Despite this major investment in security software and hardware, OPM cannot fully leverage the capability of these tools without knowing which assets must be protected, and therefore continues to remain vulnerable to security breaches.

OPM's issues with its system inventory also have a major impact on the infrastructure improvement project. Without knowing exactly how many and what type of systems need to be migrated to the new environment, there is no way to adequately plan the time and money that will be required.

Failure to maintain an up-to-date inventory and appropriately classify all systems in the environment undermines all other attempts at oversight, risk management, and securing the agency's information systems.

Failure to maintain an accurate IT inventory undermines all attempts at securing OPM's information systems.

Recommendation 1 *(Rolled Forward from 2014)*
We recommend that the OCIO develop and maintain a comprehensive inventory of all servers, databases, and network devices that reside on the OPM network.

OCIO Response:
"OCIO concurs with the recommendation. Asset inventory tools were installed on the network in FY 2015 and are being further configured to address gaps in network coverage. Additionally, network access control appliances have been installed to prevent unauthorized equipment from logging onto or being installed on the network. These tools will be aggressively implemented to provide additional assurance that a comprehensive inventory of assets is maintained."

OIG Comment:
As part of the audit resolution process, we recommend that the OCIO provide evidence to OPM's Internal Oversight and Compliance (IOC) office that is has developed a comprehensive inventory and has also implemented a process to maintain it. This statement applies to all subsequent audit recommendations that OCIO agrees to implement.

c) Systems Development Lifecycle Methodology

OPM has a history of troubled system development projects. In our opinion, the root causes of these issues are related to the lack of centralized oversight of systems development. Despite multiple attempts and hundreds of millions of dollars invested, OPM has encountered well publicized failures to modernize its retirement claims processing system. OPM has also faced struggles in modernizing its financial systems and its applications supporting the background investigation process. OPM's current infrastructure improvement project will be far more complex than these examples or anything the agency has attempted in the past.

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. Of further concern, OPM has not been following this SDLC for its infrastructure overhaul. This initiative requires a disciplined project management and systems development approach – not only for the overall project, but for the process of upgrading and migrating each individual information system.

Recommendation 2 *(Rolled Forward from 2013)*
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.

OCIO Response:
"OCIO concurs with the recommendation. An enhanced policy is being developed to update the Systems Development Life Cycle (SDLC) requirements. A plan and timeline for implementation of the policy for all Development, Modernization and Enhancement (DM&E) projects is also being developed."

B. Security Assessment and Authorization

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.

The Authorization packages reviewed as part of last year's FY 2014 FISMA audit were generally of satisfactory quality. However, 11 out of OPM's 47 major information systems had not been through the Authorization process in over three years, and several of these systems are critical to OPM's mission and/or process extremely sensitive data. Due to the volume and sensitivity of the OPM systems that were operating without an active Authorization, we classified this issue as a material weakness in the FY 2014 FISMA report.

Unfortunately, our FY 2015 FISMA audit work indicates that OPM's management of system Authorizations has deteriorated even further. In April 2015, the CIO 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. Should this moratorium on Authorizations continue throughout FY 2016, the agency will have up to 23 systems that have not been subject to a thorough security controls assessment. The justification for this action was that OPM is in the process of modernizing its IT infrastructure, and that once this modernization is complete, all systems would have to receive new Authorizations anyway.

However, the migration to OPM's new technical environment is at least five years away from completion. This is enough time for all systems to go through nearly two full Authorization cycles, and does not justify delaying the process.

It is irresponsible to allow information systems to operate indefinitely without subjecting them to a thorough security controls assessment, as OPM is doing.

Federal agencies also have the option of continuously monitoring their systems IT security controls in lieu of performing formal Authorizations every three years. However, it will also take significant time before OPM has a continuous monitoring program in place that is mature enough to mitigate the necessity of system Authorizations. OPM is planning to implement DHS's Continuous Diagnostic and Mitigation (CDM) program. However, the CDM tools are not scheduled to be installed until mid-FY 2016, and it will take some time after that for the program to mature. Although the new infrastructure and the use of CDM will certainly impact the way OPM handles Authorizations in the future, we believe that in the interim it is critical that OPM continue to subject all of its systems to this assessment process.

The Office of Management and Budget's (OMB) Circular A-130, Appendix III mandates that all Federal information systems have a valid Authorization. According to OMB, information systems should not be operating in a production environment without an Authorization, and agencies should consider shutting down systems that do not have a current and valid Authorization.

We acknowledge that the lack of an Authorization does not, by definition, mean that a system is insecure. However, it absolutely does mean that a system is at a significantly higher risk of containing unidentified security vulnerabilities. The authorization process - nearly without exception - identifies significant issues that must be addressed. If the agency does not know what weaknesses and vulnerabilities exist in its IT environment, it cannot take steps to address and remove those weaknesses, or develop a proactive and comprehensive IT security strategy.

Considering the rapidly changing pace of technology, it is irresponsible to allow these systems to operate without routinely subjecting them to a thorough security controls assessment. We continue to believe that OPM's management of system Authorizations represents a material weakness in the internal control structure of the agency's IT security program.

Recommendation 3 ***(Rolled Forward from 2014)***
We recommend that all active systems in OPM's inventory have a complete and current Authorization.

OCIO Response:
"OCIO concurs with the recommendation. OCIO made a risk-based cost-effective decision in FY 2014 to extend the authorizations for all systems in the current enterprise network. Upon

migration to the new environment, all systems will undergo a full security assessment and authorization as this constitutes a major change. As part of our analysis and planning for migration to the new infrastructure, OCIO will conduct a full assessment of the existing authorization package for systems that may remain in the legacy environment for a prolonged period of time."

OIG Comment:

Although the OCIO states that it concurs with our recommendation, its response to our draft report makes it clear that it has no intention of actually addressing this issue. We are well aware of the decision to extend Authorizations for all systems in the current enterprise network until they are migrated to the new environment. While the OCIO is presenting this extension as some sort of compensating control, we view it as the core of the problem. The OCIO could not have made a "risk-based" decision to extend the authorizations of these systems because it has not done any assessment to determine what risks actually exist within these systems. We maintain that it is irresponsible to allow these systems to operate without routinely subjecting them to a thorough security controls assessment.

Recommendation 4 *(Rolled Forward from 2014)*

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

OCIO Response:

"OCIO concurs with the recommendation. OCIO established and implemented these performance standards for the OCIO IT Project Managers (IT PM) in FY 2015. In FY 2016, OCIO will improve these standards and create a new policy to require these standards for IT PMs not positioned within OCIO."

Recommendation 5 *(Rolled Forward from 2014)*

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

OCIO Response:

"OCIO partially concurs with the recommendation. OCIO will establish a policy and process for managing authorizations to include documenting a risk-based decision by the authorizing officials to continue operations when authorizations expire."

OIG Comment:

The recommendation is that the OPM Director place consideration on shutting down information systems that do not have a current and valid Authorization – this includes a large number of systems whose Authorizations have already expired. If the Director decides to keep these systems operational even though no assessment has been done to determine what risks exist within them, then this decision should be formally documented.

C. Continuous Monitoring

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

a) Continuous Monitoring Methodology

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 5-level scale (level 1 being the least mature and effective).

We utilized this maturity model to conduct our review of OPM's information systems continuous monitoring program (ISCM). Our review determined that OPM's ISCM is currently operating at level 1, "Ad-Hoc."

Through interviews with OCIO personnel we were informed that the ISCM policies and procedures are currently being restructured to better suit the current OPM environment. These new policies and procedures will also help create a more transparent ISCM program, as the previous iteration of ISCM policies did not prove to be very effective. The policies are currently in draft form and the OCIO did not provide an estimated completion date.

We were also informed that the software platform currently used for continuous monitoring submissions and reporting has not been meeting the needs of the ISCM program. The OCIO currently has a project underway to acquire a new software package that will better integrate with OPM's environment and the requirements of the ISCM program. Defining the technology needed to support a continuous monitoring program is a critical element of CIGIE's ISCM Maturity Model.

Implementation of our recommendation will help the agency reach the next level of continuous monitoring maturity. As mentioned above, OPM is not currently performing Authorizations on many of its systems. Failure to assess the IT security controls of information systems significantly increases the risk that a system vulnerability will remain undetected and exploited.

Recommendation 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:

- Document key stakeholders and their responsibilities;
- Implement continuous monitoring submissions standardization;
- Develop requirements for personnel with significant ISCM responsibilities to have the necessary skill, knowledge, and training to complement their role;
- Develop qualitative and quantitative measures for assessing the effectiveness of the ISCM program;
- Define how ISCM information is routinely shared with top management and personnel with significant ISCM responsibilities, and
- Define the technology needed to support the ISCM program.

OCIO Response:

"OCIO partially concurs with the recommendation. We agree that policies and procedures should be developed to address the items listed in the recommendation, and will meet OPM's ISCM responsibilities in accordance with Federal laws, regulations, directives, and policies. While OPM does not have a requirement to follow the CIGIE ISCM Maturity Model, we will consider using the CIGIE ISCM Maturity Model where desirable and practicable."

OIG Comment:

While the OCIO states that it only partially agrees with the recommendation, its planned action of implementing the minimum items outlined above and leveraging the ISCM Maturity model while developing its ISCM program will address the audit recommendation.

b) Assessment of Individual System Security Controls

Not only did we determine that OPM's continuous monitoring program is inadequate, we found that many system owners are not even in compliance with it. OPM's existing policy requires all OPM operated system owners to submit evidence of continuous monitoring activities at least quarterly. Security control testing is currently required only once a year 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 20 out of 29 systems operated by OPM were subject to adequate security control continuous monitoring activity in FY 2015, and only 10 of the 17 systems operated by a contractor were subject to an adequate annual security control testing exercise.

The following program offices own information systems that failed the security control testing metric in FY 2015.

- Office of the Chief Financial Officer (two systems);
- Office of the Chief Information Officer (one system);
- Employee Services (two systems);
- Healthcare and Insurance (three systems);
- Human Resources Solutions (two systems);
- Office of the Inspector General (three systems); and
- Retirement Services (three systems).

It has been over nine years since OPM has assessed the security controls of all of its systems in a single fiscal year.

Between contractor and agency-operated information systems, only 30 out of 46 systems were subject to adequate security controls testing in FY 2015. Failure to continuously monitor and assess security controls increases the risk that agency officials are unable to make informed judgments to appropriately mitigate risks to an acceptable level.

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

Recommendation 7 (Rolled forward from 2008)

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

OCIO Response:

"OCIO concurs with the recommendation and will ensure all systems have security controls testing performed at least annually and in accordance with OPM ISCM policy."

D. 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.

a) Agency-wide security configuration policy

OPM's Information Security and Privacy Policy Handbook contains policies and procedures related to agency-wide configuration management. The handbook requires the establishment of secure baseline configurations and the monitoring and documenting of all configuration changes.

b) Configuration baselines

Our FY 2014 FISMA audit determined that OPM did not have formal baseline configurations in place for all of the operating platforms and databases used in its environment. In FY 2015, we again reviewed OPM’s progress toward establishing formal baseline configurations and determined that OPM has not made progress in implementing our recommendation. In fact it appears OPM has regressed, as we only received current baseline configurations for two operating systems ([redacted] and [redacted]), fewer than we reported in FY 2014.

Furthermore, as mentioned in Section A, Information Security Governance, OPM has not developed a comprehensive server, database and applications inventory. As a result, we are not able to independently verify whether OPM has created baseline configurations for *all* of the operating platforms it uses. However, we do know from our test work that the following operating platforms do exist in OPM’s environment, but do not have a documented baseline: [redacted], [redacted], [redacted], and [redacted].

OPM has not documented baseline configurations for all operating platforms used in its environment.

NIST SP 800-53 Revision 4 requires agencies to develop, document, and maintain a current baseline configuration of the information system. A baseline should serve as a formally approved standard outlining how to securely configure various operating platforms. Without an approved baseline, there is no standard against which actual configuration settings can be measured, increasing the risk that insecure systems exist in the operating environment.

Recommendation 8 *(Rolled Forward 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].

OCIO Response:
“OCIO partially concurs with the recommendation. While we agree that a baseline configuration should be developed for all operating platforms on the network, all of the operating platforms identified specifically in the recommendation do not exist as operating platforms on the network. OCIO will use the comprehensive asset inventory developed in conjunction with recommendation 1 to [develop] baseline configurations for the applicable operating platforms. Further, implementation of network access control appliances will prevent unauthorized devices with unauthorized operating systems from connecting to the OPM network.”

OIG Comment:
All of the operating platforms listed in the recommendation did exist in the OPM environment at some point in the past year. If these platforms are no longer used at OPM, then yes, we agree that there is no need to develop a baseline configuration for them. Once OPM has developed a comprehensive asset inventory and developed baselines for all

operating platforms that the agency does use, it should provide IOC with relevant supporting documentation.

c) United States Government Computer Baseline Configuration

OPM user workstations are built with a standard image that is compliant with the United States Government Baseline Configuration. Any deviations deemed necessary by the agency from the configurations are documented within each operating platform's baseline configuration.

We conducted an automated scan of the [redacted] standard image to independently verify compliance with OPM's baseline. Nothing came to our attention to indicate that there are weaknesses in OPM's methodology to securely configure user workstations.

d) Compliance with baselines

The OCIO uses automated scanning tools to conduct routine compliance audits on many of the operating platforms used in OPM's server environment. These tools compare the actual configuration of servers and workstations to the approved baseline configuration. However, as mentioned above, there are operating platforms used by OPM that do not have documented baseline configurations, and therefore it is impossible to subject these systems to adequate compliance audits.

NIST SP 800-53 Revision 4 requires agencies to audit activities associated with information system configurations.

Recommendation 9 *(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 8 has been completed.

OCIO Response:
"OCIO concurs with the recommendation. OCIO currently conducts routine compliance scans for existing baseline configurations and will extend scans to cover new baselines identified by remediating recommendation 8 once new operating systems and databases are identified and baselines are established."

e) Documented change management process

OPM has a documented change management process.

The OCIO has developed a Configuration Change Control Policy that outlines a formal process to approve and document all computer software and hardware changes. OPM utilizes a software application to manage, track, and document change requests.

In FY 2015, OPM acquired and implemented a software product that has the capability to detect, approve, and revert all changes made to information systems. Nothing came to our attention to indicate that there are weaknesses in OPM's software and hardware change procedures. However, as mentioned above, no software tool can be fully effective if OPM does not have a good grasp of the inventory of assets that the tool must be applied against.

f) OPM's vulnerability scanning program

We detected a variety of issues with OPM's vulnerability management program.

OPM performs some form of automated network vulnerability scanning on a bi-weekly basis. However, as mentioned throughout this report, OPM's lack of a complete system inventory makes it impossible to attest that controls of this nature are adequate and comprehensive. Furthermore, our test work identified issues with the inventory documentation that OPM *does* maintain for vulnerability scanning purposes, as we found information systems residing in areas of the network that were labeled as empty by OPM. Without a complete inventory, OPM is unable to ensure that all systems within the network environment are being scanned routinely for weaknesses.

In addition to our concerns that OPM is not conducting vulnerability scans on its entire environment, we also identified issues with the scans that do take place. OPM runs vulnerability scans using the credentials of a "service level" account. However, the scanning tool used by OPM actually requires "administrator" credentials to be fully effective. This access level is necessary to conduct the scanning, as it allows the automated tool to run a full uninhibited check for any vulnerabilities that are present within the information system. Without this level of access, an organization cannot ensure that the tool completed all of its checks and that the results from the scans are reliable. We reviewed reports that indicate numerous OPM systems are being routinely scanned with credentials that do not have sufficient access rights for a comprehensive vulnerability check.

In addition, while the OCIO has documented "accepted" weaknesses for OPM user workstations, it has not fully documented accepted weaknesses (i.e., vulnerabilities whose risk has been accepted due to a business need) for servers or databases. A recommendation related to this issue remains open from FY 2011 and is rolled forward again this year.

Finally, OPM has not implemented a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance, and we have concerns that OPM is not remediating known vulnerabilities in a timely manner.

In conclusion, we remain unable to independently attest that OPM has a mature vulnerability scanning program, and must indicate as such on the FISMA metrics provided to OMB.

Recommendation 10 *(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.

OCIO Response:
"OCIO concurs with the recommendation. OCIO will use the inventory created by remediating recommendation 1 to help ensure that vulnerability scanning is performed on all network devices and errors are corrected in a timely manner."

Recommendation 11 *(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.

OCIO Response:
"OCIO concurs with the recommendation. OCIO is working with the Department of Homeland Security (DHS), as part of the Continuous Diagnostics and Mitigation (CDM) Program, to implement and integrate the tools necessary to meet this recommendation."

Recommendation 12 (*Rolled Forward from 2011)*
We recommend that the OCIO document "accepted" weaknesses identified in vulnerability scans.

OCIO Response:
"OCIO concurs with the recommendation. OCIO will follow its standard process for documenting acceptances of risk for weaknesses identified in vulnerability scans."

OIG Comment:
We are not aware of an existing standard process for documenting acceptance of risks for weaknesses identified in vulnerability scans. If such a process exists, we recommend that the OCIO provide IOC with relevant supporting documentation.

g) Vulnerabilities identified through OIG scanning

We worked with OCIO personnel to conduct independent vulnerability scans of OPM's information systems. The results and findings of our vulnerability scanning test work is detailed below.

Unsupported software

The results of our vulnerability scans indicated that OPM's production environment contains severely out-of-date and unsupported software and operating platforms. This means that the vendor no longer provides patches, security fixes, or updates for the software.

Recommendation 13

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

OCIO Response:

"OCIO concurs with the recommendation. In FY 2016, OCIO will implement a software configuration management tool in support of Enterprise Architecture that prevents unapproved software and operating platforms from being implemented within the network environment. OCIO currently has several controls that assist in preventing unapproved software from being implemented in the network, such as requiring administrator privileges to download software."

Patch management

The OCIO has implemented a process to apply operating system patches on all devices within OPM's network on a weekly basis. The OCIO also utilizes a third party patching software management program to manage and maintain all non-operating system software. However, our scans determined that although the problems are less severe than in prior years, numerous servers are not patched in a timely fashion. Once again, OPM's lack of a comprehensive inventory makes it impossible for us or the OCIO to determine how many servers are not receiving timely patches.

Recommendation 14 *(Roll Forward from 2014)*

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.

OCIO Response:

"OCIO concurs with the recommendation. Significant progress was made in FY 2015 to apply available patches, and OCIO recognizes additional work is necessary to build a sustainable and measurable process. OCIO will continue to refine its processes for patch management."

E. 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 account and identity management within the OCIO 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) Terminated employees

OPM maintains policies related to management of user accounts for its local area network (LAN) and its mainframe environments. Both policies contain procedures for creating user accounts with the appropriate level of access as well as procedures for removing access for terminated employees.

We conducted a test comparing the current Windows and mainframe active user lists against a list of terminated employees from the past year. Nothing came to our attention to indicate that there are weaknesses in OPM's procedures for removing system access for terminated employees.

c) Multi-factor authentication with PIV

OMB Memorandum M-11-11 required all Federal information systems to be upgraded to use PIV credentials for multi-factor authentication by the beginning of FY 2012. In addition, the memorandum stated that all new systems under development must be PIV compliant prior to being made operational, and that agencies must be compliant with the memorandum prior to using technology refresh funds to complete other activities.

No OPM applications require PIV authentication.

Approximately 97 percent of laptops procured and configured by OPM require PIV authentication to log into that device. However, throughout FY 2015 there were no controls enforced that require two-factor authentication to connect other devices to the network. In other words, users could gain access to OPM's network without two-factor authentication by simply connecting with a personal device. Therefore, very few, if any, OPM users were technically required to log onto the network with two-factor PIV authentication. The only exception would be users that exclusively telework and do not have physical access to any OPM facility.

In early FY 2016 (after our draft audit report was issued), OPM began rolling out controls that would prevent non-OPM issued devices from connecting to the network. This control closes the loophole that allowed users to gain access to the network without PIV authentication.

Although OPM has made some progress in requiring PIV authentication to unlock OPM-issued devices, this does not meet 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. Even if OPM implements controls that prevent the connection of personal devices to its network, it 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 **none** of OPM's 46 major applications enforced PIV authentication. This is a critical component because without enforcing PIV authentication 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 15

We recommend that the OCIO require PIV authentication to access the OPM network.

OCIO Response:

"This recommendation has been remediated and verified by the OIG."

In early FY 2016 OPM implemented controls that enforce PIV authentication to access the network.

OIG Comment:

OPM has addressed this recommendation, no further action is required.

Recommendation 16 ***(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.

OCIO Response:

"OCIO concurs with the recommendation. OCIO will follow its planned schedule for enforcing multi-factor authentication, including the use of PIV credentials wherever feasible."

F. Incident Response and Reporting

OPM's Incident Response and Reporting Guide outlines the responsibilities of OPM's Situation Room and documents procedures for reporting all IT security events to the appropriate entities. We evaluated the degree to which OPM is following its internal procedures and FISMA requirements for reporting security incidents internally, to the United States Computer Emergency Readiness Team (US-CERT), and to appropriate law enforcement authorities.

a) Identifying and reporting incidents internally

OPM's Incident Response and Reporting Guide requires any user of the agency's IT resources to immediately notify OPM's Situation Room when IT security incidents occur. OPM reiterates this requirement in an annual mandatory IT security and privacy awareness training course.

b) Reporting incidents to US-CERT and law enforcement

OPM's Acting Director has taken steps to ensure that OIG is timely notified about any future security incidents.

OPM's Incident Response and Reporting policy states that OPM's Situation Room is responsible for sending incident reports to US-CERT on security incidents. OPM notifies US-CERT within one hour of a reportable security incident occurrence.
The Incident Response and Reporting policy also states that security incidents should be reported to law enforcement authorities, where appropriate. The OIG's Office of Investigations is part of the incident response notification distribution list, and should be notified when security incidents occur. However, the OIG was not notified on a timely basis of the major data breach that occurred in FY 2015. Failure to notify OIG investigators and auditors about the incidents in a timely manner had a negative impact on our ability to coordinate with other law enforcement organizations and conduct audit oversight activity. We brought this issue to the attention of OPM's new Acting Director, and she assured us that steps have been taken to ensure we will be directly and immediately informed of any future incidents on a timely basis.

c) Detecting, monitoring, and responding to security incidents

OPM owns a security information and event management (SIEM) tool with the technical ability to automatically detect, analyze, and correlate potential security incidents over time. We noted in the FY 2014 FISMA audit report that the tool only received event data from approximately 80 percent of major OPM information systems. In FY 2015, the SIEM now receives event data from all *known* OPM systems. We also reported last year that the tool needs to be configured to collect relevant and meaningful data so the potential security alerts contain fewer false-positives. The OPM systems currently providing data to the SIEM are over-reporting log and event data, which results in an excessive amount of data for security analysts to review. The number of alerts that security analysts must review and identify as false-positive creates a backlog that could cause a delay in identifying and responding to actual incidents. We have not been provided any evidence that this issue has been resolved.

The recent data breach was a clear indictor that OPM could improve its incident detecting and monitoring capabilities. In response to the breach, OPM procured many new security tools that are intended to better prevent and detect incidents. While it is good that OPM is attempting to improve its incident detection and monitoring capabilities, we learned that all of these tools have not been fully implemented or optimized. We believe that it is too early to tell if these tools are actually improving OPM's incident response capabilities. We will follow up on the implementation of security tools in next year's FISMA audit.

NIST 800-53 Revision 4 states that an organization must implement "an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery." The organization should also employ "automated mechanisms to support the incident handling process."

Recommendation 17 *(Rolled Forward from FY 2014)*

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.

OCIO Response:

"OCIO concurs with the recommendation. We will configure the filtering capability of the security information and event management tool to meet OPM requirements, reducing unnecessary event logs and event data where possible."

OIG Comment:

OPM addressed this recommendation in early FY 2016 (after the draft audit report was issued); no further action is required.

G. 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.

a) Agency-wide 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 2011 the OCIO organized a group comprised of several IT security professionals to fulfill the Risk Executive Function. However, as of the end of FY 2015, the group still does not have an approved charter, and therefore does not have clearly defined responsibility and authority for risk management activity at OPM. 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 a 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 18 (*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).

OCIO Response:
"OCIO partially concurs with this finding. While we believe the Risk Executive Function is important for OPM-wide risk management, OCIO can only manage risk associated with its portfolio. To that end, OCIO will use its IT governance processes and other governance processes, such as the annual Federal Financial Managers' Integrity Act (FMFIA) internal control processes, to manage risks within the OCIO portfolio."

OIG Comment:
The OCIO should continue its efforts to manage risks associated with OPM's technology portfolio, and the OPM Director should assign responsibility for implementing the elements of an agency-wide risk management program that are not covered by the OCIO.

b) 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."

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

H. 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 99 percent of OPM employees and contractors completed IT security awareness training.

Over 99 percent of OPM's employees and contractors completed the security awareness training course in FY 2015.

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 65 percent of employees identified as having significant security responsibilities completed special IT training in FY 2015.

Recommendation 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.

OCIO Response:

"OCIO concurs with this recommendation. OCIO will establish training plans for personnel with significant information security responsibility and track progress toward completion of approved classes."

I. Plan of Action & Milestones (POA&M)

A POA&M is a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for IT security weaknesses. The sections below detail OPM's effectiveness in using POA&Ms to track the agency's security weaknesses.

a) POA&Ms incorporate all known IT security weaknesses

In November 2014, the OIG issued the FY 2014 FISMA audit report with 29 audit recommendations. However, only 13 of the 29 recommendations were appropriately incorporated into the OCIO master POA&M. We have not seen how or if the remaining 16 recommendations were documented.

Failure to incorporate all known IT security weaknesses into the associated POA&M limits the agency's ability to effectively identify, assess, prioritize, and monitor the progress of the corrective efforts to remediate identified weaknesses. The following program offices failed to update their system's POA&Ms to document all known security weaknesses:

- Federal Investigative Services (three systems);
- Office of the Inspector General (one system); and
- Human Resource Solutions (one system).

Recommendation 20 *(Rolled Forward from 2014)*

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.

OCIO Response:

"OCIO concurs with the recommendation. While the vast majority of weaknesses were incorporated into the appropriate POA&M, we acknowledge that a few weaknesses were not added timely. We will update our POA&M process accordingly to assure that weaknesses are added timely in the future."

b) Prioritize Weaknesses

Each program office at OPM is required to prioritize the security weaknesses on their POA&Ms to help ensure significant IT issues are addressed in a timely manner. We verified the POA&Ms that were provided did identify and prioritize each security weakness.

c) Effective Remediation Plans and Adherence to Remediation Deadlines

Many system owners are not meeting the self-imposed remediation deadlines listed on the POA&Ms. Only 5 of OPM's 46 systems *do not* have POA&M items that are greater than 120 days overdue. We issued an audit recommendation in FY 2012 related to overdue POA&M items, and that recommendation was closed during this fiscal year based on evidence provided at the time. However, our subsequent test work determined that adherence to POA&M deadlines continues to be an issue, therefore we are issuing this recommendation once again for FY 2015. The 41 systems with overdue POA&M items are owned by:

- Office of the Chief Financial Officer (two systems);
- Office of the Chief Information Officer (nine systems);
- Employee Services (three systems);
- Federal Investigative Services (seven systems);
- Healthcare and Insurance (three systems);
- Human Resource Solutions (seven systems);
- Office of the Inspector General (four systems); and
- Retirement Services (six systems).

Recommendation 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.

OCIO Response:
"OCIO concurs with the recommendation. OCIO will create a corrective action plan for weaknesses that are more than 120 days overdue."

d) Identifying Resources to Remediate Weaknesses

Only 40 of OPM's 46 systems appropriately identify the resources needed to address POA&M weaknesses, as required by OPM's POA&M policy.

We issued an audit recommendation in FY 2014 related to resources not being identified to resolve POA&M items, and that recommendation was closed during this fiscal year based on evidence provided at that time. However, on our subsequent test work we determined that the necessary resources to remediate vulnerabilities are still not being identified on system POA&Ms for systems owned by:

- Office of the Chief Information Officer (two systems);
- Human Resource Solutions (two systems);
- Federal Investigative Services (two systems).

Recommendation 22

We recommend that all POA&Ms list the specific resources required to address each security weakness identified.

OCIO Response:

"OCIO concurs with the recommendation. OCIO will include in its POA&Ms resources required to remediate security weaknesses."

e) Supporting Documentation for Closing POA&Ms

The OCIO requires program offices to provide the evidence, or "proof of closure," that security weaknesses have been resolved before officially closing the related POA&M. When the OCIO receives a proof of closure document from the program offices for a POA&M item, an OCIO staff member will judgmentally review the documentation to determine whether or not the evidence provided was appropriate. Nothing came to our attention to indicate problems with the OCIO's process for closing POA&M items.

J. Remote Access Management

OPM has implemented policies and procedures related to authorizing, monitoring, and controlling all methods of accessing the agency's network resources from a remote location. In addition, OPM has issued agency-wide telecommuting policies and procedures, and all employees are required to sign a Rules of Behavior document that outlines their responsibility for the protection of sensitive information when working remotely.

OPM utilizes a Virtual Private Network (VPN) client to facilitate secure remote access to the agency's network environment. The OPM VPN requires the use of an individual's PIV card and password authentication to uniquely identify users. The OIG has reviewed the VPN access list to ensure that there are no shared accounts and that each user account has been tied to an individual. The agency maintains logs of individuals who remotely access the network, and the logs are reviewed on a monthly basis for unusual activity or trends.

Although there are still a small number of authorized network devices that are not compliant with PIV cards (e.g., [redacted]), these devices still require multi-factor authentication for remote access through the use of RSA tokens and password authentication.

In previous years, we discovered that remote access sessions do not terminate or lock out after 30 minutes of inactivity as required by FISMA. OPM has acknowledged the issue and stated that the weakness has not been remediated and a project is in place to address this. The scheduled completion date for the project is May 2016.

Recommendation 23 ***(Rolled Forward from 2012)***
We recommend the OCIO configure the VPN servers to terminate VPN sessions after 30 minutes of inactivity.

OCIO Response:
"OCIO concurs with the recommendation. We have thoroughly analyzed and investigated this matter. Virtual Private Network (VPN) appliances are configured and have been validated to terminate connections to the network after 30 minutes of inactivity. Some applications, agents, and software purposefully run in the background because they take a prolonged period of time to complete or because they periodically refresh data to the device. This is valid and authorized activity. Thus, OCIO believes the VPN appliance is working in accordance with the intended configuration setting."

OIG Comment:
As part of the audit resolution process, we recommend that the OCIO provide IOC with a list of the applications, agents, and software that prevents a VPN session from terminating after 30 minutes. We will work with IOC to evaluate whether it is appropriate to close this recommendation.

K. 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 2015.

a) Documenting contingency plans of individual OPM systems

We received contingency plans for 23 out of 46 information systems on OPM's master system inventory. The following program offices failed to submit adequate contingency planning documentation for one or more systems that they own:

- Office of the Chief Financial Officer (two systems);
- Office of the Chief Information Officer (six systems);
- Employee Services (three systems);
- Federal Investigative Services (one system);
- Office of Healthcare and Insurance (two systems);
- Human Resource Solutions (four systems); and

- Office of Retirement Services (five systems).

According to OPM's Information Security and Privacy Policy Handbook, "Contingency Plans shall be reviewed, updated, and tested at least annually to ensure its effectiveness." Failure to document contingency plans increases the risk that agency information systems will not be recovered in a timely manner and that critical data could be lost.

Recommendation 24 *(Rolled Forward from FY2014)*
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.

OCIO Response:
"OCIO concurs with the recommendation. OCIO will ensure contingency plans are reviewed and updated annually."

b) Testing contingency plans of individual OPM systems

OPM's Information Security Privacy and Policy Handbook requires that the contingency plan for each information system be tested at least annually using information system specific tests and exercises. We received evidence that contingency plans were tested for only 18 of OPM's 46 systems in FY 2015. This is a significant decrease from the number of systems that were tested in FY 2014. The following program offices failed to submit adequate documentation for one or more systems that they own:

- Office of the Chief Financial Officer (two systems);
- Office of the Chief Information Officer (seven systems);
- Employee Services (three systems);
- Federal Investigative Services (three systems);
- Healthcare and Insurance (two systems);
- Human Resources Solutions (six systems); and
- Retirement Services (five systems).

Of the contingency plan tests we did receive, we noted improved quality in documentation as it relates to the analysis or "lessons learned" section of the report. However, due to the significantly low number of tests received, we cannot conclude that OPM has improved the overall quality and consistency of its contingency plan testing methodology.

NIST SP 800-34 Revision 1 states that following a contingency plan test, "results and lessons learned should be documented and reviewed by test participants and other personnel as appropriate. Information collected during the test and post-test reviews that improve plan effectiveness should be incorporated into the contingency plan."

<u>**Recommendation 25 (*Rolled Forward from 2008)***</u>

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.

<u>OCIO Response:</u>

"OCIO concurs with the recommendation. OCIO will test contingency plans annually."

c) Testing contingency plans of OPM general support systems

In the FY 2011 FISMA audit report we recommended that the OCIO implement a centralized (agency-wide) approach to contingency plan testing. The intent of the recommendation is to ensure that all elements of the general support systems are subject to a full functional disaster recovery test each year. This recommendation has been remediated in FY 2015 and is now closed.

OPM conducted tests of its general support system contingency plans.

Many OPM systems reside on one of the agency's general support systems. The OCIO typically conducts a full recovery test at the backup location of the Enterprise Server Infrastructure general support system (i.e., the mainframe and associated systems) on an annual basis. In FY 2015 a successful functional contingency plan test was conducted and documented that involved OPM's Enterprise Server Infrastructure and the LAN/WAN general support system.

L. <u>Contractor Systems</u>

We evaluated the methods that the OCIO and various program offices use to maintain oversight of their systems operated by contractors on behalf of OPM.

a) Contractor system documentation

OPM's master system inventory indicates that 17 of the agency's 46 major applications are operated by a contractor.

In the past, the OCIO maintained a separate spreadsheet documenting interfaces between OPM and contractor-operated systems and the related Interconnection Security Agreements (ISA). However, we were told that the spreadsheet was not maintained in FY 2015. 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.

The OCIO did not provide evidence that they track Memoranda of Understanding/Agreement (MOU/A). These documents outline the terms and conditions for sharing data and information resources in a secure manner. The OCIO should track MOU/As to ensure that valid agreements are in place for each documented ISA.

Recommendation 26 (*Rolled Forward from 2014)*

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

OCIO Response:

"OCIO concurs with the recommendation. OCIO will update its processes for identifying, controlling, and maintaining interconnections and their associated documentation."

Recommendation 27 (*Rolled Forward from 2014)*

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

OCIO Response:

Recommendation 27 was combined with Recommendation 26 in the draft audit report. The OCIO response to Recommendation 26 applies to this recommendation as well.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], Lead IT Auditor-In-Charge

[redacted], Lead IT Auditor

[redacted], Lead IT Auditor

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], IT Auditor

[redacted], Group Chief

Appendix I

Status of Prior OIG Audit Recommendations

The tables below outline the current status of prior audit recommendations issued in FY 2014 by the Office of the Inspector General.

Report No. 4A-CI-00-14-016: FY 2014 Federal Information Security Management Act Audit, issued November 12, 2014

Rec #	Original Recommendation	Recommendation History	Current Status
1	We recommend that OPM implement a centralized information security governance structure where all information security practitioners, including designated security officers, report to the CISO. Adequate resources should be assigned to the OCIO to create this structure. Existing designated security officers who report to their program offices should return to their program office duties. The new staff that reports to the CISO should consist of experienced information security professionals.	Roll-forward from OIG Reports: • 4A-CI-00-10-019 Recommendation 4, • 4A-CI-00-11-009 Recommendation 2, • 4A-CI-00-12-016 Recommendation 1, and • 4A-CI-00-13-021 Recommendation 1	CLOSED 9/30/2015
2	We recommend that the OCIO develop a plan and timeline to enforce the new SDLC policy to all of OPM's system development projects.	Roll-forward from OIG Report: • 4A-CI-00-13-021 Recommendation 2,	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 2
3	We recommend that all active systems in OPM's inventory have a complete and current Authorization.	Recommendation new in FY 2014	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 3
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.	Recommendation new in FY 2014	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 4
5	We recommend that the OPM Director consider shutting down information systems that do not have a current and valid Authorization.	Recommendation new in FY 2014	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 5
6	We recommend that the OCIO 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).	Roll-Forward from OIG Report: • 4A-CI-00-11-009 Recommendation 6, • 4A-CI-00-12-016 Recommendation 2, and • 4A-CI-00-13-021 Recommendation 3	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 18

Status of Prior OIG Audit Recommendations

7	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].	Recommendation new in 2014	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 8
8	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 7 has been completed.	Recommendation new in 2014	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 9
9	We recommend the OCIO implement technical controls that prevent configuration changes without proper documentation and approvals.	Recommendation new in 2014	CLOSED 8/26/2015
10	We recommend that the OCIO develop and maintain a comprehensive inventory of all servers, databases, and network devices that reside on the OPM network.	Recommendation new in 2014	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 1
11	We recommend that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.	Recommendation new in 2014	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 10
12	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.	Recommendation new in 2014	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 11
13	We recommend that the OCIO document "accepted" weaknesses identified in vulnerability scans.	Roll-forward from OIG Reports: • 4A-CI-00-11-009 Recommendation 9, • 4A-CI-00-12-016 Recommendation 4, and • 4A-CI-00-13-021 Recommendation 6	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 12
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.	Recommendation new in 2014	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 14
15	We recommend that the OCIO expand the capabilities of the ENSOC to ensure that security incidents from all OPM-operated information systems are centrally analyzed and correlated.	Recommendation new in 2014	CLOSED: 9/30/2015

Status of Prior OIG Audit Recommendations

16	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.	Recommendation new in 2014	CLOSED: 11/06/15
17	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.	Recommendation new in 2014	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 20
18	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.	Roll-forward from OIG Reports: • 4A-CI-00-12-016 Recommendation 8 and • 4A-CI-00-13-021 Recommendation 8	CLOSED: 1/16/15 Reissued as 4A-CI-00-15-011 Recommendation 21
19	We recommend that all POA&Ms list the specific resources required to address each security weakness identified.	Recommendation new in 2014	CLOSED: 11/12/14 Reissued as 4A-CI-00-15-011 Recommendation 22
20	We recommend the OCIO configure the VPN servers to terminate VPN sessions after 30 minutes of inactivity.	Roll-forward from OIG Reports: 4A-CI-00-12-016 Recommendation 10 and 4A-CI-00-13-021 Recommendation 10	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 23
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.	Roll-forward from OIG Reports: 4A-CI-00-12-016 Recommendation 11 and 4A-CI-00-13-021 Recommendation 11	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 16
22	We recommend that the OCIO expand its continuous monitoring program to include mandatory continuous monitoring for contractor-operated systems and implementation of the DHS Continuous Diagnostic and Mitigation program as outlined in the OCIO's continuous monitoring strategy.	Recommendation new in 2014	CLOSED: 9/30/2015

Status of Prior OIG Audit Recommendations

23	We recommend that OPM ensure that an annual test of security controls has been completed for all systems.	Roll-forward from OIG Reports: • 4A-CI-00-08-022 Recommendation 1, • 4A-CI-00-09-031 Recommendation 6, • 4A-CI-00-10-019 Recommendation 10, • 4A-CI-00-11-009 Recommendation 11, • 4A-CI-00-12-016 Recommendation 14, and • 4A-CI-00-13-021 Recommendation 13	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 7
24	We recommend that the OCIO ensure that all of OPM's major systems have contingency plans in place and are reviewed and updated annually.	Recommendation new in 2014	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 24
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 eight systems that were not subject to adequate testing in FY 2014.	Roll-forward from OIG Reports: • 4A-CI-00-08-022 Recommendation 2, • 4A-CI-00-09-031 Recommendation 9, • 4A-CI-00-10-019 Recommendation 30, • 4A-CI-00-11-009 Recommendation 19, • 4A-CI-00-12-016 Recommendation 15, and • 4A-CI-00-13-021 Recommendation 14	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 25
26	We recommend that the OCIO implement and document a centralized (agency-wide) approach to contingency plan testing.	Roll-forward from OIG Reports: • 4A-CI-00-11-009 Recommendation 21, • 4A-CI-00-12-016 Recommendation 16, and • 4A-CI-00-13-021 Recommendation 15	CLOSED: 9/30/2015
27	We recommend that the OCIO identify agency systems that reside in a public cloud and document those systems on the master system inventory.	Recommendation new in 2014	CLOSED: 11/12/2014
28	We recommend that the OCIO ensure that all ISAs are valid and properly maintained.	Recommendation new in 2014	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 26
29	We recommend that the OCIO ensure that a valid MOU/A exists for every interconnection.	Recommendation new in 2014	OPEN: Rolled-forward as Report 4A-CI-00-15-011 Recommendation 27

Appendix II

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington DC 20415

Chief Information Officer

October 22, 2015

MEMORANDUM FOR: [redacted]
Chief, Information Systems Audit Group
Office of the Inspector General

FROM: DONNA K. SEYMOUR
Chief Information Officer

SUBJECT: Office of the Chief Information Officer Response to the Office of the Inspector General Federal Information Security Modernization Act Audit – FY 2015 (Report No. 4A-CI-00-15-011)

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report for the Fiscal Year (FY) 2015 Federal Information Security Modernization Act (FISMA) Audit for the U.S. Office of Personnel Management (OPM). The OIG comments are valuable to the office of the Chief Information Officer (OCIO) 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.

As a practice we have established in our monthly meetings, OCIO intends to track these recommendations in our dashboards to facility the aggressive pursuit of remediations, and we will provide updates at each meeting. I am proud that OCIO has closed 77% of the recommendations for the FY 2007 through FY 2014 OIG FISMA Audits, as well as OIG system audits. We believe this progress during the past year demonstrates that OPM takes the recommendations seriously and is focused on protecting its data and information technology (IT) systems.

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

Recommendation 1 ***(Rolled Forward from 2014)***
We recommend that the OCIO develop and maintain a comprehensive inventory of all servers, databases, and network devices that reside on the OPM network.

CIO Response: OCIO concurs with the recommendation. Asset inventory tools were installed on the network in FY 2015 and are being further configured to address gaps in network coverage. Additionally, network access control appliances have been installed to prevent unauthorized equipment from logging onto or being installed on the network. These tools will be aggressively implemented to provide additional assurance that a comprehensive inventory of assets is maintained.

Recommendation 2 *(Rolled Forward from 2013)*
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.

CIO Response: OCIO concurs with the recommendation. An enhanced policy is being developed to update the Systems Development Life Cycle (SDLC) requirements. A plan and timeline for implementation of the policy for all Development, Modernization and Enhancement (DM&E) projects is also being developed.

Recommendation 3 *(Rolled Forward from 2014)*
We recommend that all active systems in OPM's inventory have a complete and current Authorization.

CIO Response: OCIO concurs with the recommendation. OCIO made a risk-based cost-effective decision in FY 2014 to extend the authorizations for all systems in the current enterprise network. Upon migration to the new environment, all systems will undergo a full security assessment and authorization as this constitutes a major change. As part of our analysis and planning for migration to the new infrastructure, OCIO will conduct a full assessment of the existing authorization package for systems that may remain in the legacy environment for a prolonged period of time.

Recommendation 4 *(Rolled Forward from 2014)*
We recommend that the performance standards of all OPM system owners be modified to include a requirement related to FISMA compliance for the information systems they own. At a minimum, system owners should be required to ensure that their systems have valid Authorizations.

CIO Response: OCIO concurs with the recommendation. OCIO established and implemented these performance standards for the OCIO IT Project Managers (IT PM) in FY 2015. In FY 2016, OCIO will improve these standards and create a new policy to require these standards for IT PMs not positioned within OCIO.

Recommendation 5 *(Rolled Forward from 2014)*
We recommend that the OPM Director consider shutting down information systems that do not have a current and valid Authorization.

CIO Response: OCIO partially concurs with the recommendation. OCIO will establish a policy and process for managing authorizations to include documenting a risk-based decision by the authorizing officials to continue operations when authorizations expire.

Recommendation 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:

- Document key stakeholders and their responsibilities;
- Implement continuous monitoring submissions standardization;
- Develop requirements for personnel with significant ISCM responsibilities to have the necessary skill, knowledge, and training to complement their role;
- Develop qualitative and quantitative measures for assessing the effectiveness of the ISCM program;
- Define how ISCM information is routinely shared with top management and personnel with significant ISCM responsibilities, and
- Define the technology needed to support the ISCM program.

CIO Response: OCIO partially concurs with the recommendation. We agree that policies and procedures should be developed to address the items listed in the recommendation, and will meet OPM's ISCM responsibilities in accordance with Federal laws, regulations, directives, and policies. While OPM does not have a requirement to follow the CIGIE ISCM Maturity Model, we will consider using the CIGIE ISCM Maturity Model where desirable and practicable.

Recommendation 7 ***(Rolled forward from 2008)***
We recommend that OPM ensure that an annual test of security controls has been completed for all systems.

CIO Response: OCIO concurs with the recommendation and will ensure all systems have security controls testing performed at least annually and in accordance with OPM ISCM policy.

Recommendation 8 ***(Rolled Forward 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].

CIO Response: OCIO partially concurs with the recommendation. While we agree that a baseline configuration should be developed for all operating platforms on the network, all of the operating platforms identified specifically in the recommendation do not exist as operating platforms on the network. OCIO will use the comprehensive asset inventory developed in conjunction with recommendation 1 to baseline configurations for the applicable operating platforms. Further, implementation of network access control appliances will prevent unauthorized devices with unauthorized operating systems from connecting to the OPM network.

Recommendation 9 ***(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 8 has been completed.

CIO Response: OCIO concurs with the recommendation. OCIO currently conducts routine compliance scans for existing baseline configurations and will extend scans to cover new baselines identified by remediating recommendation 8 once new operating systems and databases are identified and baselines are established.

Recommendation 10 *(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.

CIO Response: OCIO concurs with the recommendation. OCIO will use the inventory created by remediating recommendation 1 to help ensure that vulnerability scanning is performed on all network devices and errors are corrected in a timely manner.

Recommendation 11 *(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.

CIO Response: OCIO concurs with the recommendation. OCIO is working with the Department of Homeland Security (DHS), as part of the Continuous Diagnostics and Mitigation (CDM) Program, to implement and integrate the tools necessary to meet this recommendation.

Recommendation 12 (*Rolled Forward from 2011)*
We recommend that the OCIO document “accepted” weaknesses identified in vulnerability scans.

CIO Response: OCIO concurs with the recommendation. OCIO will follow its standard process for documenting acceptances of risk or weaknesses identified in vulnerability scans.

Recommendation 13
We recommend the OCIO implement a process to ensure that only supported software and operating platforms are utilized within the network environment.

CIO Response: OCIO concurs with the recommendation. In FY 2016, OCIO will implement a software configuration management tool in support of Enterprise Architecture that prevents unapproved software and operating platforms from being implemented within the network environment. OCIO currently has several controls that assist in preventing unapproved software from being implemented in the network, such as requiring administrator privileges to download software.

Recommendation 14 *(Roll Forward from 2014)*
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.

CIO Response: OCIO concurs with the recommendation. Significant progress was made in FY 2015 to apply available patches, and OCIO recognizes additional work is necessary to build a sustainable and measurable process. OCIO will continue to refine its processes for patch management.

Recommendation 15
We recommend that the OCIO require PIV authentication to access the OPM network.

CIO Response: This recommendation has been remediated and verified by the OIG.

Recommendation 16 *(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.

CIO Response: OCIO concurs with the recommendation. OCIO will follow its planned schedule for enforcing multi-factor authentication, including the use of PIV credentials wherever feasible.

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

CIO Response: OCIO concurs with the recommendation. We will configure the filtering capability of the security information and event management tool to meet OPM requirements, reducing unnecessary event logs and event data where possible.

Recommendation 18 (*Rolled Forward from 2011)*
We recommend that the OCIO 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).

CIO Response: OCIO partially concurs with this finding. While we believe the Risk Executive Function is important for OPM-wide risk management, OCIO can only manage risk associated with its portfolio. To that end, OCIO will use its IT governance processes and other governance processes, such as the annual Federal Financial Managers' Integrity Act (FMFIA) internal control processes, to manage risks within the OCIO portfolio.

Recommendation 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.

CIO Response: OCIO concurs with this recommendation. OCIO will establish training plans for personnel with significant information security responsibility and track progress toward completion of approved classes.

Recommendation 20 *(Rolled Forward from 2014)*
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.

CIO Response: OCIO concurs with the recommendation. While the vast majority of weaknesses were incorporated into the appropriate POA&M, we acknowledge that a few weaknesses were not added timely. We will update our POA&M process accordingly to assure that weaknesses are added timely in the future.

Recommendation 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.

CIO Response: OCIO concurs with the recommendation. OCIO will create a corrective action plan for weaknesses that are more than 120 days overdue.

Recommendation 22

We recommend that all POA&Ms list the specific resources required to address each security weakness identified.

CIO Response: OCIO concurs with the recommendation. OCIO will include in its POA&Ms resources required to remediate security weaknesses.

Recommendation 23 *(Rolled Forward from 2012)*

We recommend the OCIO configure the VPN servers to terminate VPN sessions after 30 minutes of inactivity.

CIO Response: OCIO concurs with the recommendation. We have thoroughly analyzed and investigated this matter. Virtual Private Network (VPN) appliances are configured and have been validated to terminate connections to the network after 30 minutes of inactivity. Some applications, agents, and software purposefully run in the background because they take a prolonged period of time to complete or because they periodically refresh data to the device. This is valid and authorized activity. Thus, OCIO believes the VPN appliance is working in accordance with the intended configuration setting.

Recommendation 24 *(Rolled Forward from FY2014)*

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.

CIO Response: OCIO concurs with the recommendation. OCIO will ensure contingency plans are reviewed and updated annually.

Recommendation 25 (*Rolled Forward from 2008)*

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.

CIO Response: OCIO concurs with the recommendation. OCIO will test contingency plans annually.

Recommendation 26
We recommend the OCIO ensure that a valid ISA and MOU/A exists for every interconnection.

CIO Response: OCIO concurs with the recommendation. OCIO will update its processes for identifying, controlling, and maintaining interconnections and their associated documentation.

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

Copy to:
Janet Barnes, Director, Internal Oversight and Control

Appendix III

Inspector General

Section Report

2015

Annual FISMA Report

Office of Personnel Management

Section 1: Continuous Monitoring Management

1.1 **Utilizing the ISCM maturity model definitions, please assess the maturity of the organization's ISCM program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the ISCM program overall.**

1.1.1 **Please provide the D/A ISCM maturity level for the People domain.**

Ad Hoc (Level 1)

1.1.2 **Please provide the D/A ISCM maturity level for the Processes domain.**

Ad Hoc (Level 1)

1.1.3 **Please provide the D/A ISCM maturity level for the Technology domain**

Ad Hoc (Level 1)

1.1.4 **Please provide the D/A ISCM maturity level for the ISCM Program Overall.**

Ad Hoc (Level 1)

1.2 **Please provide any additional information on the effectiveness of the organization's Information Security Continuous Monitoring Management Program that was not noted in the maturity model above.**

Comments

Comments: OPM's ISCM policies and procedures are currently being restructured to better suit the current OPM environment. These newpolicies and procedures will also help create a more transparent ISCM program, as the previous iteration of ISCM policies did notprove to be very effective. The policies are currently in draft form and the OCIO did not provide an estimated completion date. We were also informed that the software platform currently used for continuous monitoring submissions and reporting has not beenmeeting the needs of the ISCM program. The OCIO currently has a project underway to acquire a new software package that willbetter integrate with OPM's environment and the requirements of the ISCM program. Defining the technology needed to support acontinuous monitoring program is a critical element of CIGIE's ISCM Maturity Model.

Section 2: Configuration Management

2.1 **Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

No

Section 2: Configuration Management

2.1.1 **Documented policies and procedures for configuration management.**

Yes

2.1.2 **Defined standard baseline configurations.**

No

Comments: OPM does not have formal baseline configurations for all of the operating platforms and databases used in its environment.

2.1.3 **Assessments of compliance with baseline configurations.**

No

Comments: The OCIO uses automated scanning tools to conduct routine compliance audits on many of the operating platforms used in OPM's server environment. However, as mentioned above, there are operating platforms used by OPM that do not have documented baseline configurations, and therefore it is impossible to subject these systems to adequate compliance audits.

2.1.4 **Process for timely (as specified in organization policy or standards) remediation of scan result findings.**

No

Comments: OPM has not implemented a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance, and we have concerns that OPM is not remediating known vulnerabilities in a timely manner.

2.1.5 **For Windows-based components, USGCB secure configuration settings are fully implemented (when available), and any deviations from USGCB baseline settings are fully documented.**

Yes

2.1.6 **Documented proposed or actual changes to hardware and software baseline configurations.**

Yes

Section 2: Configuration Management

2.1.7 Implemented software assessing (scanning) capabilities (NIST SP 800-53: RA-5, SI- 2).

Yes

Comments: OPM performs some form of automated network vulnerability scanning on a bi-weekly basis. However, OPM's lack of a complete system inventory makes it impossible to attest that controls of this nature are adequate and comprehensive. In addition to our concerns that OPM is not conducting vulnerability scans on its entire environment, we also identified issues with the scans that do take place. OPM runs vulnerability scans using the credentials of a "service level" account. However,the scanning tool used by OPM actually requires "administrator" credentials to be fully effective. We reviewed reports that indicate numerous OPM systems are being routinely scanned with credentials that do not have sufficient access rights for a comprehensive vulnerability check.

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

No

Comments: OPM has not implemented a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance, and we have concerns that OPM is not remediating known vulnerabilities in a timely manner.

2.1.9 Patch management process is fully developed, as specified in organization policy or standards, including timely and secure installation of software patches (NIST SP 800-53: CM-3, SI-2).

No

Comments: The OCIO has implemented a process to apply operating system patches on all devices within OPM's network on a weeklybasis. The OCIO also utilizes a third party patching software management program to manage and maintain allnon-operating system software. However, our scans determined that although the problems are less severe than in prioryears, numerous servers are not patched in a timely fashion. Once again, OPM's lack of comprehensive inventory makes it impossible for us or the OCIO to determine how many servers are not receiving timely patches.

2.2 Please provide any additional information on the effectiveness of the organization's Configuration Management Program that was not noted in the questions above.

N/A

Section 2: Configuration Management

2.3 Does the organization have an enterprise deviation handling process and is it integrated with an automated scanning capability?

Yes

2.3.1 Is there a process for mitigating the risk introduced by those deviations? A deviation is an authorized departure from an approved configuration. As such it is not remediated but may require compensating controls to be implemented.

Yes

Section 3: Identity and Access Management

3.1 Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and which identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes?

Yes

3.1.1 Documented policies and procedures for account and identity management (NIST SP 800-53: AC-1).

Yes

3.1.2 Identifies all users, including Federal employees, contractors, and others who access organization systems (HSPD 12, NIST SP 800-53, AC-2).

Yes

3.1.3 Organization has planned for implementation of PIV for logical 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).

Yes

3.1.4 Organization has planned for implementation of 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).

Yes

Comments: Approximately 97 percent of laptops procured and configured by OPM require PIV authentication to log into that device.However, throughout FY 2015 there were no controls enforced that require two-factor authentication to connect otherdevices to the network. In addition, none of OPM’s 46 major applications enforced PIV authentication. OPM has a plan in place to implement PIV authentication for all systems, but it will be a multi-year project.

Section 3: Identity and Access Management

3.1.5 Ensures that the users are granted access based on needs and separation-of-duties principles.

Yes

3.1.6 Distinguishes hardware assets that have user accounts (e.g., desktops, laptops, servers) from those without user accounts (e.g. IP phones, faxes, printers).

Yes

3.1.7 Ensures that accounts are terminated or deactivated once access is no longer required according to organizational policy.

Yes

3.1.8 Identifies and controls use of shared accounts.

Yes

3.2 Please provide any additional information on the effectiveness of the organization’s Identity and Access Management Program that was not noted in the questions above.

N/A

Section 4: Incident Response and Reporting

4.1 Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

4.1.1 Documented policies and procedures for detecting, responding to, and reporting incidents (NIST SP 800-53: IR-1).

Yes

4.1.2 Comprehensive analysis, validation, and documentation of incidents.

Yes

4.1.3 When applicable, reports to US-CERT within established timeframes (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).

Yes

4.1.4 When applicable, reports to law enforcement and the agency Inspector General within established timeframes.

Yes

Section 4: Incident Response and Reporting

4.1.5 Responds to and resolves incidents in a timely manner, as specified in organization policy or standards, to minimize further damage (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).

Yes

4.1.6 Is capable of correlating incidents.

Yes

4.1.7 Has sufficient incident monitoring and detection coverage in accordance with government policies (NIST SP 800-53, 800-61; OMB M-07-16, M-06-19).

Yes

4.2 Please provide any additional information on the effectiveness of the organization's Incident Management Program that was not noted in the questions above.

N/A

Section 5: Risk Management

5.1 Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

No

Comments: In FY 2011 the OCIO organized a group comprised of several IT security professionals to fulfill the Risk ExecutiveFunction. However, as of the end of FY 2015, the group still does not have an approved charter, and therefore does nothave clearly defined responsibility and authority for risk management activity at OPM. In addition, the 12 primary elementsof 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 a risk assessment, maintaining a risk registry, communicating the agency-wide risks down to the system owners, and ensuring proper authorization of agency information systems.

5.1.1 Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST SP 800-37, Rev. 1.

No

Comments: OPM has not taken steps to address risk management from an organization perspective, and has not conducted an agency-wide risk assessment.

Section 5: Risk Management

5.1.2 Addresses risk from a mission and business process perspective and is guided by the risk decisions from an organizational perspective, as described in NIST SP 800- 37, Rev. 1.

No

Comments: OPM has not implemented a process to address risk from an organization perspective (5.1.1), therefore organization risk cannot guide mission and business process risk management.

5.1.3 Addresses risk from an information system perspective and is guided by the risk decisions from an organizational perspective and the mission and business perspective, as described in NIST SP 800-37, Rev.1.

No

Comments: OPM has not implemented a process to address risk from an organization perspective (5.1.1), therefore organization risk cannot guide information system risk management.

5.1.4 Has an up-to-date system inventory.

No

Comments: OPM has not developed a comprehensive server, database and applications inventory. Without a reliable inventory, OPM'sconfiguration management controls are not effective, as there is no assurance that they are being enforced in the entiretechnical environment. OPM has historically maintained a fragmented and decentralized technical infrastructure that is spreadover six data centers and is maintained by different organizations within the agency . Over the past several years, the agencyhas procured a variety of tools to help automate efforts to secure the OPM network . However, our audit determined that all of these tools are not being utilized to their fullest capacity, as the agency was having difficulty implementing and enforcing the new controls on all endpoints of the decentralized network.

5.1.5 Categorizes information systems in accordance with government policies.

Yes

5.1.6 Selects an appropriately tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.

Yes

5.1.7 Implements the approved set of tailored baseline security controls specified in metric 5.1.6.

Yes

Section 5: Risk Management

5.1.8 Assesses the security 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.

No

Comments: OPM's existing policy requires all OPM operated system owners to submit evidence of continuous monitoring activities atleast quarterly. Security control testing is currently required only once a year for OPM systems operated by a contractor.We determined that only 20 out of 29 systems operated by OPM were subject to adequate security control continuous monitoring activity in FY 2015, and only 10 of the 17 systems operated by a contractor were subject to an adequate annual security control testing exercise.

5.1.9 Authorizes information system operation 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.

No

Comments: Due to the volume and sensitivity of the OPM systems that were operating without an active Authorization, we classified thisissue as a material weakness in the FY 2014 FISMA report. Unfortunately, our FY 2015 FISMA audit work indicates thatOPM's management of system Authorizations has deteriorated even further. In April 2015, the CIO issued a memorandumthat granted an extension of the previous Authorizations for all systems whose Authorization had already expired, and forthose scheduled to expire through September 2016. Should this moratorium on Authorizations continue, the agency willhave up to 23 systems that have not been subject to a thorough security controls assessment. It is irresponsible to allowthese systems to operate without routinely subjecting them to a thorough security controls assessment. We continue to believe that OPM's management of system Authorizations represents a material weakness in the internal control structure of the agency's IT security program.

5.1.10 Information-system-specific risks (tactical), mission/business-specific risks, and organizational-level (strategic) risks are communicated to appropriate levels of the organization.

No

Comments: OPM has not implemented a process to address risk from an organization perspective (5.1.1), therefore it is not possible to measure whether risks are communicated to the appropriate levels of the organization.

5.1.11 Senior officials are briefed on threat activity on a regular basis by appropriate personnel (e.g., CISO).

Yes

Section 5: Risk Management

5.1.12 **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.**

Yes

5.1.13 **Security authorization package contains system security plan, security assessment report, POA&M, accreditation boundaries in accordance with government policies for organization information systems (NIST SP 800-18, 800-37).**

No

Comments: The Authorization packages that do exist are of acceptable quality, but many OPM systems do not currently have an active Authorization (see 5.1.9).

5.1.14 **The organization has an accurate and complete inventory of their cloud systems, including identification of FedRAMP approval status.**

Yes

5.1.15 **For cloud systems, the organization can identify the security controls, procedures, policies, contracts, and service level agreements (SLA) in place to track the performance of the Cloud Service Provider (CSP) and manage the risks of Federal program and personal data stored on cloud systems.**

No

Comments: OPM cannot effectively track the performance of Cloud Service Providers because many of the existing contracts do not contain appropriate language.

5.2 **Please provide any additional information on the effectiveness of the organization's Risk Management Program that was not noted in the questions above.**

N/A

Section 6: Security Training

6.1 **Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

Section 6: Security Training

6.1.1 Documented policies and procedures for security awareness training (NIST SP 800-53: AT-1).

Yes

6.1.2 Documented policies and procedures for specialized training for users with significant information security responsibilities.

Yes

6.1.3 Security training content based on the organization and roles, as specified in organization policy or standards.

Yes

6.1.4 Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other organization users) with access privileges that require security awareness training.

Yes

6.1.5 Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other organization users) with significant information security responsibilities that require specialized training.

No

Comments: OPM employees with significant information security responsibilities are required to take specialized security training inaddition to the annual awareness training. The OCIO has developed a table outlining the security training requirements forspecific job roles. The OCIO uses a spreadsheet to track the security training taken by employees that have been identifiedas having security responsibility. Only 65 percent of employees identified as having significant security responsibilities have completed special IT training in FY 2015.

6.1.6 Training material for security awareness training contains appropriate content for the organization (NIST SP 800-50, 800-53).

Yes

6.2 Please provide any additional information on the effectiveness of the organization's Security Training Program that was not noted in the questions above.

N/A

Section 7: Plan Of Action & Milestones (POA&M)

Section 7: Plan Of Action & Milestones (POA&M)

7.1 **Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

7.1.1 **Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and that require remediation.**

Yes

7.1.2 **Tracks, prioritizes, and remediates weaknesses.**

Yes

7.1.3 **Ensures remediation plans are effective for correcting weaknesses.**

Yes

7.1.4 **Establishes and adheres to milestone remediation dates and provides adequate justification for missed remediation dates.**

No

Comments: Many system owners are not meeting the self-imposed remediation deadlines listed on the POA&Ms. Only 5 of OPM's 46 systems do not have POA&M items that are greater than 120 days overdue.

7.1.5 **Ensures resources and ownership are provided for correcting weaknesses.**

No

Comments: Only 40 of OPM's 46 systems appropriately identify the resources needed to address POA&M weaknesses, as required by OPM's POA&M policy.

7.1.6 **POA&Ms include security weaknesses discovered during assessments of security controls and that require remediation (do not need to include security weakness due to a risk- based decision to not implement a security control) (OMB M-04-25).**

No

Comments: In November 2014, the OIG issued the FY 2014 FISMA audit report with 29 audit recommendations. However, only 13of the 29 recommendations were appropriately incorporated into the OCIO master POA&M. We have not seen how or if the remaining 16 recommendations were documented.

Section 7: Plan Of Action & Milestones (POA&M)

7.1.7 Costs associated with remediating weaknesses are identified in terms of dollars (NIST SP 800-53: PM-3; OMB M-04-25).

Yes

7.1.8 Program officials report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53:CA-5; OMB M-04-25).

Yes

7.2 Please provide any additional information on the effectiveness of the organization's POA&M Program that was not noted in the questions above.

N/A

Section 8: Remote Access Management

8.1 Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

8.1.1 Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST SP 800-53: AC-1, AC-17).

Yes

8.1.2 Protects against unauthorized connections or subversion of authorized connections.

Yes

8.1.3 Users are uniquely identified and authenticated for all access (NIST SP 800-46, Section 4.2, Section 5.1).

Yes

8.1.4 Telecommuting policy is fully developed (NIST SP 800-46, Section 5.1).

Yes

8.1.5 Authentication mechanisms meet NIST SP 800-63 guidance on remote electronic authentication, including strength mechanisms.

Yes

Section 8: Remote Access Management

8.1.6 Defines and implements encryption requirements for information transmitted across public networks.

Yes

8.1.7 Remote access sessions, in accordance with OMB M-07-16, are timed-out after 30 minutes of inactivity, after which re-authentication is required.

No

Comments: Remote access sessions do not terminate after 30 minutes of inactivity.

8.1.8 Lost or stolen devices are disabled and appropriately reported (NIST SP 800-46, Section 4.3; US-CERT Incident Reporting Guidelines).

Yes

8.1.9 Remote access rules of behavior are adequate in accordance with government policies (NIST SP 800-53, PL-4).

Yes

8.1.10 Remote-access user agreements are adequate in accordance with government policies (NIST SP 800-46, Section 5.1; NIST SP 800-53, PS-6).

Yes

8.2 Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.

N/A

8.3 Does the organization have a policy to detect and remove unauthorized (rogue) connections?

Yes

Comments: This control was implemented in early FY 2016.

Section 9: Contingency Planning

9.1 Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

Section 9: Contingency Planning

9.1.1 **Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST SP 800-53: CP-1).**

Yes

9.1.2 **The organization has incorporated the results of its system's Business Impact Analysis and Business Process Analysis into the appropriate analysis and strategy development efforts for the organization's Continuity of Operations Plan, Business Continuity Plan, and Disaster Recovery Plan (NIST SP 800-34).**

Yes

9.1.3 **Development and documentation of division, component, and IT infrastructure recovery strategies, plans, and procedures (NIST SP 800-34).**

Yes

9.1.4 **Testing of system-specific contingency plans.**

No

Comments: We received evidence that contingency plans were tested for only 18 of OPM's 46 systems in FY 2015. This is a significant decrease from the number of systems that were tested in FY 2014.

9.1.5 **The documented BCP and DRP are in place and can be implemented when necessary (FCD1, NIST SP 800-34).**

Yes

9.1.6 **Development of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

9.1.7 **Testing or exercising of BCP and DRP to determine effectiveness and to maintain current plans.**

Yes

9.1.8 **After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34).**

Yes

9.1.9 **Alternate processing sites are not subject to the same risks as primary sites. Organization contingency planning program identifies alternate processing sites for systems that require them (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

Section 9: Contingency Planning

9.1.10 Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53).

Yes

9.1.11 Contingency planning that considers supply chain threats.

Yes

9.2 Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.

N/A

Section 10: Contractor Systems

10.1 Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including for organization systems and services residing in a cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?

Yes

10.1.1 Documented policies and procedures for information security oversight of systems operated on the organization's behalf by contractors or other entities (including other government agencies), including organization systems and services residing in a public, hybrid, or private cloud.

Yes

10.1.2 The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and compliant with FISMA requirements, OMB policy, and applicable NIST guidelines (NIST SP 800-53: CA-2).

No

Comments: Only 10 of the 17 systems operated by a contractor were subject to an adequate annual security control testing exercise.

10.1.3 A complete inventory of systems operated on the organization's behalf by contractors or other entities, (including other government agencies), including organization systems and services residing in public, hybrid, or private cloud.

Yes

10.1.4 The inventory identifies interfaces between these systems and organization- operated systems (NIST SP 800-53: PM-5).

Yes

Section 10: Contractor Systems

10.1.5 **The organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates.**

No

Comments: In the past, the OCIO maintained a separate spreadsheet documenting interfaces between OPM and contractor-operatedsystems and the related Interconnection Security Agreements (ISA). However, we were told that the spreadsheet was not maintained in FY 2015.

10.1.6 **The inventory of contractor systems is updated at least annually.**

Yes

10.2 **Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.**

N/A

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 --

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage (*http://www.opm.gov/our-inspector-general*), caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.