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

Final Audit Report

Subject:

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT FY 2013

Report No. 4A-CI-00-13-021

Date: November 21, 2013

--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, 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.

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT
FY 2013

WASHINGTON, D.C.

Report No. 4A-CI-00-13-021

Date: November 21, 2013

Michael R. Esser
Assistant Inspector General
for Audits

--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, 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

U.S. OFFICE OF PERSONNEL MANAGEMENT

FEDERAL INFORMATION SECURITY
MANAGEMENT ACT AUDIT
FY 2013

WASHINGTON, D.C.

Report No. 4A-CI-00-13-021

Date: November 21, 2013

This final audit report documents the Office of Personnel Management's (OPM) continued efforts to manage and secure its information resources.

Over the past several years, the Office of the Chief Information Officer (OCIO) made noteworthy improvements to OPM's IT security program. However, we are concerned that these efforts have recently stalled due to resource limitations.

In the FY 2007 FISMA report, we noted a material weakness related to the lack of IT security policies and procedures. In FY 2009, we expanded the material weakness to include the lack of a centralized security management structure necessary to implement and enforce IT security policies.

Little progress was made in the subsequent years to address these issues. However, in FY 2012, the OPM Director issued a memo mandating the centralization of IT security duties to a team of Information System Security Officers (ISSO) that report to the OCIO. This change was a major milestone in addressing the material weakness.

However, as of the end of FY 2013, the centralized ISSO structure has only been partially implemented. The OCIO had filled three ISSO positions and assigned security responsibility for 17 of the agency's 47 information systems to these individuals. The OCIO has a plan to hire enough ISSOs to manage the security of all 47 systems, but this plan continues to be hindered by budget restrictions.

We acknowledge that the existing ISSOs are effectively performing security work for the limited number of systems they manage, but there are still many OPM systems that have not been assigned to an ISSO. The findings in this audit report highlight the fact that OPM's decentralized governance structure continues to result in many instances of non-compliance with FISMA requirements. Therefore, we are again reporting this issue as a material weakness for FY 2013.

In addition to the issues described above, we noted the following controls in place and opportunities for improvement:

- The Security Assessment and Authorization packages completed in FY 2013 appeared to be an improvement over Authorizations completed in prior years, and the packages present a more uniform approach to IT security.
- The OCIO has implemented risk management procedures at a system-specific level, but has not developed an agency-wide risk management methodology.
- The OCIO has implemented an agency-wide information system configuration management policy and has established configuration baselines for all operating platforms used by the agency, with the exception of [redacted]. In addition, [redacted] are not routinely scanned for compliance with configuration baselines.
- The OCIO routinely conducts vulnerability scans of production servers, and has improved its capability to track outstanding vulnerabilities. However, the OCIO has not documented accepted weaknesses for servers or databases.
- The OCIO has implemented a process to apply operating system patches on all devices within OPM's network on a weekly basis.
- The OCIO has developed thorough incident response capabilities, but does not have a centralized network security operations center to continuously monitor security events.
- Our review of Plans of Action and Milestones (POA&M) indicated that many system owners are not meeting the self-imposed remediation deadlines listed on the POA&Ms. In addition we noted that the owners of 10 systems have not identified the resources needed to address POA&M weaknesses, as required by OPM's POA&M policy.
- The OCIO enforces the use of two-factor authentication for remote access, but Virtual Private Network sessions do not [redacted], as required by OPM's Information Technology Security FISMA Procedures.
- OPM is not compliant with Office of Management and Budget Memorandum M-11-11, as no OPM systems require two-factor authentication using PIV credentials.
- The OCIO has developed the ability to detect unauthorized devices connected to the OPM network.

- The OCIO has taken steps toward implementing a continuous monitoring program at OPM; however, this project remains a work in progress.
- The IT security controls were adequately tested for only 34 of 47 information systems in OPM's inventory.
- The contingency plans were adequately tested for only 40 of 47 information systems in OPM's inventory.
- There is not a coordinated contingency plan/disaster recovery test between OPM's various general support systems.
- OPM maintains an adequate security capital planning and investment program for information security.
- OPM is continuing its efforts to reduce the unnecessary use of Social Security Numbers.

Contents

Page

Introduction

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 (FISMA). FISMA 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. 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.

Background

FISMA requirements pertain to all information systems supporting the operations and assets of an agency, including those systems currently in place or planned. The requirements also pertain to information technology (IT) resources owned and/or operated by a contractor supporting agency systems.

FISMA reemphasizes the Chief Information Officer's strategic, agency-wide security responsibility. At 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 Communication issued the Fiscal Year (FY) 2013 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.

Objectives

Our overall objective was to evaluate OPM's security program and practices, as required by FISMA. Specifically, we reviewed the status of the following areas of OPM's IT security program in accordance with DHS's FISMA IG reporting requirements:

- Risk Management;
- Configuration Management;
- Incident Response and Reporting Program;
- Security Training Program;
- Plans of Action and Milestones (POA&M) Program;
- Remote Access Program;
- Identity and Access Management;
- Continuous Monitoring Program;

- Contingency Planning Program;
- Agency Program to Oversee Contractor Systems; and
- Agency Security Capital Planning Program.

In addition, we evaluated the status of OPM's IT security governance structure, an area that has represented a material weakness in OPM's IT security program in prior FISMA audits.

We also audited the security controls of three major applications/systems at OPM (see Scope and Methodology for details of these audits), and audited the OCIO's use of a Common Security Controls Catalog. We also 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 2013.

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:

- USA Staffing (Report No. 4A-HR-00-13-024, issued June 21, 2013);
- Personnel Investigations Processing System (Report No. 4A-IS-00-13-022, issued June 24, 2013);
- Serena Business Manager (Report No. 4A-CI-00-13-023, issued July 19, 2013); and
- Common Security Controls Catalog (report No. 4A-CI-00-13-036, issued October 10, 2013).

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 testing 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 include:

- DHS Office of Cybersecurity and Communications FY 2013 Inspector General Federal Information Security Management Act Reporting Instructions;
- OPM Information Technology Security and Privacy Handbook;
- OPM Information Technology Security FISMA Procedures;
- OPM Security Assessment and Authorization Guide;
- 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;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- National Institute of 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;
- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems;
- NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories;
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities;
- 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 May through September 2013 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 the "Results" section of this report.

Results

The sections below detail the results of our FY 2013 FISMA audit of OPM's IT Security Program. Many recommendations were issued in prior FISMA audits and are rolled forward from the 2012 FISMA audit (Report No. 4A-CI-00-12-016).

I. 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. For many years, we have reported increasing concerns about the state of OPM's information security governance. In the FY 2007 FISMA report, we issued a material weakness related to the lack of IT policies and procedures. In FY 2009, we expanded the material weakness to include the lack of a centralized security management structure necessary to implement and enforce IT policies.

We also have growing concerns about OPM's ability to manage major system development projects and the decentralized nature of the agency's technical operating environment.

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

a) Information security management structure

Information system security at OPM has historically been managed by individual Designated Security Officers (DSO) that report to the various program offices that own major computer systems. Many of these DSOs are not certified IT security professionals, and are performing DSO duties as collateral responsibility to another full-time position.

In FY 2011, the OCIO updated its IT security and privacy policies, but information security was still managed by DSOs that were not qualified to implement the new policies. In FY 2012, the OPM Director issued a memo mandating the transfer of IT security duties from the decentralized program office DSOs to a centralized team of Information System Security Officers (ISSO) that report to the OCIO. This change was a major milestone in addressing the material weakness.

However, as of the end of FY 2013, the centralized ISSO structure has only been partially implemented. The OCIO has filled three ISSO positions and assigned security responsibility for 17 of the agency's 47 information systems to these individuals. The OCIO has a plan to hire enough ISSOs to manage the security of all 47 systems, but this plan continues to be hindered by budget restrictions.

The existing ISSOs are effectively performing security work for the limited number of systems they manage, but there are still many OPM systems that have not been assigned to an ISSO. The findings in this audit report highlight the fact that OPM's decentralized governance structure continues to result in many instances of non-compliance with FISMA requirements. Specifically, the sections below related to continuous monitoring, contingency planning, and POA&Ms all describe specific weaknesses that could be improved with the full implementation of a centralized security governance structure. Therefore, we are again classifying this issue as a material weakness for FY 2013.

Recommendation 1 (*Rolled-Forward from 2010*)

We recommend that OPM implement a centralized information security governance structure where all information security practitioners, including designated security officers, report to the Chief Information Security Officer (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.

OCIO Response:

"A CIO initiated Memo directing the centralization of the security responsibilities of Designated Security Officers (DSO) in the Office of Chief Information Security Officer (CISO) was issued by the OPM Director on August, 2012 with an effective date of October 1, 2012. The CIO has already hired three Information System Security Officers with professional IT security experience and certifications and recruitment of an additional one is in progress for a total of four. The initial set of systems has been transitioned to ISSOs for security management and we expect to have all OPM systems under CISO security management once funding for additional professional security staff becomes available."

OIG Reply:

We acknowledge the progress that the OCIO has made in implementing a centralized IT security structure, and will continue to monitor its effectiveness in FY 2014.

b) Systems development lifecycle methodology

OPM has a history of troubled system development projects. In our opinion, the root cause of these issues relates to the lack of central policy and oversight of systems development. Many system development projects at OPM have been initiated and managed by program offices with limited oversight or interaction with the OCIO. These program office managers do not always have the appropriate background in project management or information technology systems development.

The OCIO has recently published a new system development lifecycle (SDLC) policy, which is a significant first step in implementing a centralized SDLC methodology at OPM. However, policy alone will not improve the historically weak SDLC management capabilities of OPM.

The new policy is currently only applicable to OPM's 11 major IT investments and is not actively enforced on other IT projects. However, it is imperative that the OCIO make it a priority to enforce this new policy to all system development projects. The failure of OPM's Service Credit system was an example of a system development project that did not meet the criteria of a major investment, but when it failed there were serious consequences for the agency – not financial, but impactful to stakeholders and embarrassing in terms of media exposure and political scrutiny.

The new SDLC policy does incorporate several prior OIG recommendations related to a centralized review process of system development projects. We also recommended that the OCIO develop a team with the proper project management and system development expertise to oversee new system development projects. Through this avenue, the OCIO should review SDLC projects at predefined checkpoints, and provide strict guidance to ensure that program office management is following OPM's SDLC policy and is employing proper project management techniques to ensure a successful outcome for all new system development projects.

Recommendation 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.

OCIO Response:

"The OPM SDLC is being applied to OPM's major investment projects. In FY14, a plan with timelines will be developed to enforce the SDLC policy for applicable system development projects."

OIG Reply:

We acknowledge the steps that the OCIO is taking to expand the enforcement of the SDLC policy, and reiterate that we believe the policy should be enforced to all OPM IT projects.

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

II. Security Assessment and Authorization

System certification is a comprehensive assessment that attests that a system's security controls are meeting the security requirements of that system, and accreditation is the official management decision to authorize operation of an information system and accept its risks. OPM's process of certifying a system's security controls is referred to as Security Assessment and Authorization (Authorization.)

In FY 2011, the OCIO published updated procedures and templates designed to improve the overall Authorization process and dedicated resources to facilitating system Authorizations. The new process resulted in a noticeable improvement in the agency's Security Authorization packages and in FY 2012, we observed a continued improvement in the Authorization packages completed under this new process. This improvement has continued through FY 2013, and we believe this is due to the more rigorous review process through which the OCIO is requiring program offices to comply with policies, procedures, and the use of templates.

We reviewed the full Authorization packages of 15 systems that were subject to an Authorization during FY 2013. The quality of all packages appeared to be an improvement over Authorizations completed in prior years, and the packages present a more uniform approach to IT security.

III. Risk Management

NIST SP 800-37 Revision 1 "Guide for Applying the Risk Management Framework to Federal Information Systems" 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 Risk Executive Function comprised of several IT security professionals. However, as of the end of FY 2012, the 12 primary elements of the Risk Executive Function as described in NIST SP 800-39 were 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, and communicating the agency-wide risks down to the system owners. Although the OCIO improved in assessing risk at the individual system level (see Security Assessment and Authorization section II, above), the OCIO was not fully managing risk at an organization-wide level.

As of FY 2013, no further changes have been implemented to address organization-wide risk.

Recommendation 3 (*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).

OCIO Response:

"We will continue to assess the Risk Executive Function per NIST Special Publication 800-39 and to explore and make suggestions for implementing this function. The risk executive function will have agency wide authority and responsibility for assessing risk across all OPM Program Offices and to advise senior management on risk management strategies."

b) System specific risk management and annual security controls testing

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 new Authorization process. In addition, OPM policy requires each major information system to be subject to routine security controls testing.

IV. Configuration Management

The sections below detail the controls that the OCIO has in place to manage the technical configuration of OPM servers 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

In FY 2013, OPM put forth significant effort to document and implement new baseline configurations for critical applications, servers, and workstations.   At the end of the fiscal year, the OCIO had established baselines and/or build sheets for the following operating systems:

- Windows Internet Explorer 8,
- Windows XP,
- Windows 7, and
- Windows 2008 R2.

The OCIO is currently developing new baselines for [redacted].

NIST SP 800-53 Revision 3 control CM-2 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 4

We recommend that the OCIO develop and implement a baseline configuration for [redacted].

OCIO Response:

"We are working to standardize operating systems and applications throughout the environment. Over the past year, all Windows and Linux operating systems, as well as Microsoft SQL have been given approved baseline images. We will continue to improve our processes and develop and implement configuration baselines for [redacted]."

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 Windows 7 standard image to independently verify compliance with the appropriate guideline and 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 the majority of operating platforms used in OPM's server environment. These tools compare the actual configuration of servers and workstations to the approved baseline configuration. In FY 2013, the OCIO implemented a process to routinely scan [redacted]. However, these scans are not performed using an approved [redacted] because, as mentioned above, current baseline configurations for these platforms are in development.

NIST SP 800-53 Revision 3 control CM-3 requires agencies to audit activities associated with information system configurations.

Recommendation 5

We recommend that the OCIO conduct routine compliance audits on [redacted] with the OPM baseline configuration once they have been reviewed, updated, and approved.

OCIO Response:

"We concur with this recommendation and will implement the recommendation on the approved baseline configuration."

e) Software and hardware change management

The OCIO has developed a Configuration Change Control Policy that outlines a formal process to approve and document all computer software and hardware changes. The OCIO utilizes a software application to manage and maintain all computer software and hardware change control documentation.

We reviewed evidence indicating that the OCIO is adequately following this policy and is thoroughly documenting all system changes. Nothing came to our attention to indicate that there are weaknesses in OPM's change management process.

f) Vulnerability scanning

OPM's Network Management Group (NMG) performs monthly vulnerability scans of all servers using automated scanning tools. A daily security advisory report is generated that details the most vulnerable servers and workstations, and these reports are sent to system owners so they can remediate the identified weaknesses.

NMG has documented accepted weaknesses for OPM user workstations; however, it has not fully documented weaknesses for servers or databases (i.e., vulnerability scan findings that are justified by a business need). This recommendation remains open from FY 2011 and is rolled forward in FY 2013.

Recommendation 6 (*Rolled Forward from 2011*)

We recommend that the OCIO document "accepted" weaknesses identified in vulnerability scans.

<u>OCIO Response:</u>

"We concur with this recommendation and will implement the recommendation in FY-14."

g) Patch management

The OCIO has implemented a process to apply operating system patches on all devices within OPM's network on a weekly basis. In FY 2013, the OCIO began utilizing a third party patching software management program to manage and maintain all non-operating system software.

We conducted vulnerability scans on a sample of servers and determined that servers are appropriately patched. Nothing came to our attention to indicate that there are weaknesses in OPM's patch management process.

V. 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 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 the information provided in the Incident Response and Reporting Guide in an annual mandatory IT security and privacy awareness training course. In addition, OPM also uses three different software tools to prevent and detect intrusions and malware in the agency's network.

The OCIO has processes in place to quickly respond to all reported security incidents. Our FY 2012 FISMA report indicated that there were several incidents in that fiscal year that were not appropriately reported to the Situation Room. In response, the OCIO provided documentation indicating that it had improved the annual incident response training. This training appears to have improved incident response reporting, as we are unaware of any incidents that were not appropriately reported in FY 2013.

b) Reporting incidents to US-CERT and law enforcement

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 is notified when security incidents occur.

c) Correlating and monitoring security incidents

OPM owns a software product with the technical ability to compare and correlate security incidents over time. However, the correlation features of these tools are not being fully utilized at this time. This tool receives event data from approximately 80 percent of all major OPM systems. Furthermore, OPM does not have a consistent and unified process to monitor and analyze all security incidents. Some incidents cannot be fully investigated due to inconsistent logging practices across systems, and inefficiencies created by program offices running separate monitoring tools on their systems.

The OCIO's NMG is in the process of establishing an Enterprise Network Security Operations Center (ENSOC) that will provide continuous centralized support for OPM's security incident prevention/management, performance analysis, fault resolution, maintenance coordination, configuration management, security management, system monitoring, network monitoring, alert escalation, problem resolution bridge coordination, and incident response. Although we agree that the proposed ENSOC will greatly improve OPM's incident management capabilities and overall security of the agency, the OCIO continues to face resource limitations that hinder the full implementation of the ENSOC.

Recommendation 7 (Rolled Forward from 2012)

We recommend that the OCIO establish a centralized network security operations center with the ability to monitor security events for all major OPM systems.

OCIO Response:

"A centralized monitoring center is established with first level alerting and monitoring for the servers, and network appliances within the major OPM sites. Work has begun on incorporating application and database monitoring and compliance. We will continue to evaluate and look at cost effective ways to implement this recommendation."

VI. 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, peer-to-peer software, and the roles and responsibilities of users.

Over 98 percent of OPM's employees and over 99 percent of contractors completed the security awareness training course in FY 2013.

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. Of employees with significant security responsibilities, 96 percent completed specialized IT security training in FY 2013.

VII. Plan of Action and Milestones

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

The OIG FY 2012 FISMA audit contained 18 audit recommendations; we verified that all 18 recommendations were appropriately incorporated into the OCIO master POA&M.

Although only 34 of OPM's 47 major systems provided the OIG with annual security controls tests (see section X, below), we were able to verify that all security weaknesses identified during these tests were incorporated into the appropriate system's POA&M.

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

All system owners are required to create action steps (milestones) to effectively remediate specific weaknesses identified on POA&Ms. Our review of the POA&Ms indicated that system owners are appropriately listing milestones and target completion dates on their POA&Ms.

However, our review also indicated that many system owners are not meeting the self-imposed remediation deadlines listed on the POA&Ms. Of OPM's 47 major systems, 22 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. The recommendation was closed during this fiscal year because the OCIO provided updated corrective action plans for multiple systems. However, we are re-issuing the recommendation because overdue POA&M items now exist for nearly half of OPM systems.

Recommendation 8

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:

"The CIO dedicated resources to this task and has successfully closed a majority of POA&Ms that are over 120 days old and will continue to work with program offices to reduce or close those that are outstanding and to develop formal Corrective Action Plans. Most POA&Ms that are over 120 days have dependencies such as funding that is not available or coordination issues with external entities who often are not ready to implement the required changes."

OIG Reply:

We acknowledge that resource limitations will often impact the amount of time required to address a system weakness. However, the remediation deadlines on the POA&M's are self-imposed and should be reasonable to meet. Additional training for systems owners on establishing appropriate POA&M deadlines may help resolve this issue.

d) Identifying resources to remediate weaknesses

We noted that the owners of 10 systems have not identified the resources needed to address POA&M weaknesses, as required by OPM's POA&M policy.

Recommendation 9 (Rolled Forward from 2012)

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

OCIO Response:

"This recommendation has been largely implemented for program offices with open POA&Ms. We will continue to work with program offices to ensure that the 'resources required' for POA&Ms are identified and documented."

e) OCIO tracking and reviewing POA&M activities on a quarterly basis

System owners are required to submit a POA&M to the OCIO on a quarterly basis. In addition, 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 employee will judgmentally review the documentation to determine whether or not the evidence provided was appropriate.

We selected one closed POA&M item from each of 10 OPM systems and reviewed the proof of closure documentation provided by the program offices. The 10 systems were judgmentally selected from the 47 OPM systems. We determined that adequate proof of closure was provided for all 10 systems tested. The results of the sample test were not projected to the entire population.

VIII. 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 portion of authorized network devices that are not compliant with PIV cards (e.g., iPads), these devices still require multi-factor authentication for remote access through the use of RSA tokens and password authentication.

We did note one problem related to the FISMA requirement that a remote access session be [redacted]. We connected workstations to OPM's VPN server and [redacted] but neither VPN session was [redacted] The OCIO is in the process of conducting research on possible secondary controls to mitigate this issue and believes this is a major flaw in the vendor's design.

Recommendation 10 (Rolled Forward from 2012)

We recommend the OCIO configure the VPN servers to [redacted]

OCIO Response:

"All technological controls are in place and we believe there is a flaw in a vendor's design that will require an out of band patch to repair. We have narrowed the problem to a fault within the UDP connection to the client and we are working with the vendor, Cisco Systems to get this resolved."

IX. 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 an access test comparing the current LAN active user list against a list of terminated employees from the past year. Nothing came to our attention to indicate that there are weaknesses in OPM's access termination management process.

c) Multi-factor authentication with PIV

OMB Memorandum M-11-11 requires 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.

In FY 2012, the OCIO began an initiative to require PIV authentication to access the agency's network. As of the end of FY 2013, 30 percent of OPM workstations require PIV authentication for access to the OPM network. However, none of the agency's 47 major applications require PIV authentication.

Recommendation 11 (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:

"We have developed and are in the process of implementing plans for multi-factor PIV authentication for compliance with OMB M-11-11. A major segment of the users on our network infrastructure are using PIV authentication. In FY-14 we will continue to work with program offices to implement PIV authentication for major systems."

d) Unauthenticated network devices

In prior FISMA audits, we have recommended that the OCIO implement an automated process to detect non-approved devices connected to OPM's network. The OCIO has purchased a Network Access Controller (NAC) that will govern access to network resources. The NAC has the ability to identify all devices on the network and deny access to unauthenticated devices.

Nothing came to our attention to indicate that there are weaknesses in OPM's controls over unauthenticated devices.

X. Continuous Monitoring Management

The following sections detail OPM's controls related to continuous monitoring of the security state of its information systems.

a) Continuous monitoring policy and procedures

OPM's Information Security and Privacy Policy Handbook states that the security controls of all systems must be continuously monitored and assessed to ensure continued effectiveness. In FY 2012, the OCIO published an addendum to the Information Security and Privacy Policy which states that it is the ISSO/DSOs responsibility to assess all security controls in an information system. The addendum also states that continuous monitoring security reports must be provided to ITSP at least semiannually.

As stated in section I above, the ISSO function has not been fully established at OPM. Our FY 2012 FISMA report stated that many of the current DSOs do not have the technical skills or the resources required to adequately monitor the information security controls of their systems. Therefore, we continue to believe that OPM's continuous monitoring policies and procedures cannot be adequately implemented until the agency's centralized ISSO function has been fully established.

b) Continuous monitoring strategy

The OCIO developed a concept of operations document and a continuous monitoring program implementation "roadmap" that describes the stages and timeline for implementing a full continuous monitoring program at OPM. While the initial stages of implementation began in FY 2012, full implementation of the plan is not scheduled to be completed until FY 2015. The OCIO achieved the FY 2013 milestones outlined in the roadmap which included semiannual reporting for all OPM-operated systems. The next stage in the OCIO's plan involves quarterly submissions for High impact systems, more frequent controls testing for all systems, and further implementation of automated tools. Implementation of this stage is scheduled to be completed during FY 2014.

Recommendation 12

We recommend that the OCIO expand its continuous monitoring program to include quarterly submissions for High impact systems, more frequent controls testing for all systems, and further implementation of automated tools as outlined in the Information Security Continuous Monitoring Roadmap.

OCIO Response:

"We have made significant progress implementing Continuous Monitoring at OPM and will continue to expand the program over a 2 year period into FY-15 subject to availability of funds. We plan to implement this specific set of recommendations from the draft report."

c) Annual assessment of security controls

OPM policy requires all OPM system owners to submit evidence of continuous monitoring activities at least semiannually (in March and September).

We requested the security test results for all OPM-operated systems for both submissions in order to review them for quality and consistency. However, we were only provided testing documentation for 20 out of the 26 major OPM-operated systems.

At this time, security controls testing for contractor-operated systems is still only required annually. A review of contractor system security control testing (see section XII, below) indicates that only 14 out of 21 contractor-operated systems were tested in this fiscal year.

Between contractor- and agency-operated information systems, only 34 out of 47 systems were subject to adequate security controls testing in FY 2013.
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 six years since all OPM systems were subject to an adequate annual security controls test. OPM's decentralized approach to IT security has traditionally placed responsibility on the various program offices to test the security controls of their systems. The OCIO's lack of authority over these program offices has contributed to the inadequate security controls testing of the agency's information systems. We are optimistic that the quality and consistency of security controls tests will improve with the full implementation of the OCIO's centralized ISSO structure and with the shift to semi-annual continuous monitoring submissions.

Recommendation 13 (Rolled Forward from 2008)

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

OCIO Response:

"We continue to make progress with security controls testing in FY-2013 and expect to have test plans and results for all systems in FY-2014. Security controls testing will be a major part of our continuous monitoring program that is currently being implemented."

XI. 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 2013.

a) Documenting contingency plans of individual OPM systems

We verified that contingency plans exist for all 47 production systems on OPM's master system inventory.

In prior OIG FISMA audits, we noted that the quality and consistency of contingency plans varied greatly between OPM's various systems. As a result, the OCIO developed a contingency plan template that all system owners are now required to use. The new template closely follows the guidance of NIST SP 800-34, Contingency Planning Guide for Federal Information Systems.

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 40 of 47 systems in FY 2013.

Of the contingency plan tests we did receive, we continue to notice inconsistency in the quality of the documentation produced for various OPM systems. One of the main areas of inconsistency relates to the analysis or "lessons learned" section of the report. NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, states that an after action report should "include background information about the exercise, documented observations made by the facilitator and data collector, and recommendations for enhancing the IT plan that was exercised."

Several after action reports we reviewed did not include summarized results or lessons learned. Without a thoroughly documented after action report, system owners will not know how to improve the contingency plan in order to be better prepared for a disruptive event.

Recommendation 14 (*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 tested for the systems that were not subject to adequate testing in FY 2013 as soon as possible.

OCIO Response:

"We will continue making progress working with program offices on contingency plan testing in FY-14. Due to the current shortage of funding for all ISSOs, the CISO must still rely on decentralized DSOs for support to complete the testing. This has caused delays in implementation and coordination."

c) Testing contingency plans of OPM general support systems

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. However, no test was performed in FY 2013 due to planned major changes in OPM's technical environment. OPM purchased a new mainframe and successfully failed-over all production data and applications from the old mainframe to the new one. However, the fail-over did not take place in the backup location.

One of OPM's other major general support system, the LAN/WAN general support system, is not routinely subject to a full functional disaster recovery test. Only select LAN/WAN systems that impact or interface with the mainframe environment are tested annually in conjunction with the mainframe disaster recovery test. Other critical applications such as the email server were successfully tested in FY 2013.

NIST SP 800-53 Revision 3 states that FIPS 199 "high" systems should be subject to "a full recovery and reconstitution of the information system to a known state as part of contingency plan testing." Without full functional routine testing of all OPM general support systems, there is a risk that OPM systems will not be successfully recovered in the event of a disaster.

In the FY 2011 FISMA audit report we recommended that the OCIO implement a centralized (agency-wide) approach to contingency plan testing. We were informed that a single synchronized functional test is not feasible due to logistical and resource limitations. However, 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 can be remediated if each general support system is subject to a full functional test each year, even if it must be broken into a series of smaller tests.

Recommendation 15 (Rolled Forward from 2011)

We recommend that the OCIO implement and document a centralized (agency-wide) approach to contingency plan testing.

OCIO Response:

"We will continue efforts to centralize contingency plan testing in FY-14 with the goal of implementing this recommendation."

XII. Contractor Systems

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.

1. Contractor system documentation

OPM's master system inventory indicates that 21 of the agency's 47 major applications are operated by a contractor. The OCIO also maintains a separate spreadsheet documenting interfaces between OPM and contractor-operated systems and the related Interconnection Security Agreements.

2. Contractor system oversight

The OPM Information Security and Privacy Policy Addendum states that "It is the responsibility of the OPM system owner to ensure systems or services hosted by non-OPM organizations comply with OPM information security and privacy policies." The handbook addendum also states that "OPM System Owners must ensure that an annual security controls assessment is performed by a government employee or an independent third party at the site where contracted information technology services are rendered."

We requested the annual security control tests for contractor-operated systems in order to review them for quality and consistency. However, we were only provided testing documentation for 14 out of the 21 systems (see section X above for the related recommendation. Failure to complete the annual security controls test increases the risk that agency officials are unable to make informed judgments to appropriately mitigate risks to an acceptable level.

XIII. Security Capital Planning

NIST SP 800-53 Revision 3, control SA-2, Allocation of Resources, states that an organization needs to determine, document, and allocate the resources required to protect information systems as part of its capital planning and investment control process.

OPM's Information Security and Privacy Policy Handbook contains policies and procedures to ensure that information security is addressed in the capital planning and investment process. The OCIO uses the Integrated Data Collection, a replacement to the Exhibit 53B, to record information security resources allocation and submits this information annually to OMB.

Nothing came to our attention to indicate that OPM does not maintain an adequate capital planning and investment program for information security.

XIV. Follow-up of Prior OIG Audit Recommendations

All open audit recommendations issued prior to 2012 were rolled forward into one of the recommendations in the FY 2012 OIG FISMA audit report (Report 4A-CI-00-12-016) FY 2012 recommendations that were not remediated by the end of FY 2013 are rolled forward with a new recommendation number in this FY 2013 OIG FISMA audit report.

The prior sections of this report evaluate the current status of many 2012 recommendations. However, there is one additional 2012 recommendation that has not yet been addressed in this report because the related topic was not part of the FY 2013 FISMA reporting instructions. The current status of this recommendation is below.

a) **4A-CI-00-12-016 Recommendation 16 (*Rolled Forward from 2008*)**

We recommend that OPM continue its efforts to eliminate the unnecessary use of SSNs in accordance with OMB Memorandum M-07-16.

FY 2013 Status

The OCIO has an ongoing plan to reduce and eventually eliminate the unnecessary use of SSNs in its major information systems. However, resource limitations prevented them from completing this task in FY 2013. This recommendation remains open and is rolled forward in FY 2013.

Recommendation 16 (*Rolled Forward from 2008)*

We recommend that OPM continue its efforts to eliminate the unnecessary use of SSNs in accordance with OMB Memorandum M-07-16.

OCIO Response:

"Significant work was done to eliminate the unnecessary use of social security numbers (SSN) including development of a consolidated Action Plan and eliminating them from USAJOBS and the PMF systems. In FY-14, the Privacy Officer will update the action plan and schedule a pilot project with Retirement Services to review business processes to determine how SSNs usage can be reduced. Note that this recommendation requires funding for agency-wide implementation."

Major Contributors to this Report

This audit report was prepared by the U.S. Office of Personnel Management, Office of Inspector General, Information Systems Audits Group. The following individuals participated in the audit and the preparation of this report:

- Lewis F. Parker, Deputy Assistant Inspector General for Audits
- [redacted], Chief, Information Systems Audits Group
- [redacted] Lead IT Auditor
- [redacted], IT Auditor
- [redacted], IT Auditor
- [redacted] IT Auditor

Appendix I

Status of Prior OIG Audit Recommendations

The table below outlines the current status of prior audit recommendations issued in FY 2012 by the Office of the Inspector General.

Report No. 4A-CI-00-12-016: FY 2012 Federal Information Security Management Act Audit, issued November 5, 2012

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 and • 4A-CI-00-11-009 Recommendation 2	OPEN: Rolled-forward as Report 4A-CI-00-13-021 Recommendation 1
2	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	OPEN: Rolled-forward as Report 4A-CI-00-13-021Recommendation 3
3	We recommend that the OCIO implement a process to routinely audit [redacted] for compliance with the approved OPM baseline configuration.	Recommendation new in FY 2012	CLOSED: 6/20/2013
4	We recommend that the OCIO document "accepted" weaknesses identified in vulnerability scans.	Roll-Forward from OIG Report: • 4A-CI-00-11-009 Recommendation 9	OPEN: Rolled-forward as Report 4A-CI-00-13-021Recommendation 6
5	We recommend that the OCIO implement a process to timely patch (or remove altogether) third party applications on its servers.	Recommendation new in FY 2012	CLOSED: 9/25/2013

6	We recommend that the OCIO establish a centralized network security operations center with the ability to monitor security events for all major OPM systems.	Recommendation new in FY 2012	OPEN: Rolled-forward as Report 4A-CI-00-13-021Recommendation 7
7	We continue to recommend that the OCIO ensure that all employees with significant information security responsibility take meaningful and appropriate specialized security training on an annual basis.	Roll-Forward from OIG Reports: • 4A-CI-00-10-019 Recommendation 16, and • 4A-CI-00-11-009 Recommendation 10	CLOSED 9/26/2013
8	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.	Recommendation new in FY 2012	CLOSED: 2/26/2013 Reissued as 4A-CI-00-13-021Recommendation 8
9	We recommend that all POA&Ms list the specific resources required to address each security weakness identified.	Recommendation new in FY 2012	OPEN: Rolled-forward as Report 4A-CI-00-13-021Recommendation 9
10	We recommend the OCIO configure the VPN servers to terminate VPN sessions after 30 minutes of inactivity.	Recommendation new in FY 2012	OPEN: Rolled-forward as Report 4A-CI-00-13-021Recommendation 10
11	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.	Recommendation new in FY 2012	OPEN: Rolled-forward as Report 4A-CI-00-13-021Recommendation 11
12	We recommend that the OCIO implement an automated process to detect unauthenticated network devices.	Roll-Forward from OIG Reports: • 4A-CI-00-10-019 Recommendation 25, and • 4A-CI-00-11-009 Recommendation 16	CLOSED: 9/25/2013
13	We recommend that the OCIO expand its continuous monitoring program to include a reporting process at the system-level, and implement automated tools and metric reporting for OPM as outlined in the Information Security Continuous Monitoring Roadmap	Recommendation new in FY 2012	CLOSED: 9/25/2013
14	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, and • 4A-CI-00-11-009 Recommendation 11	OPEN: Rolled-forward as Report 4A-CI-00-13-021Recommendation 13

15	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 2012.	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, and • 4A-CI-00-11-009 Recommendation 19	OPEN: Rolled-forward as Report 4A-CI-00-13-021Recommendation 14
16	We recommend that the OCIO implement and document a centralized (agency-wide) approach to contingency plan testing.	Roll-Forward from OIG Report: • 4A-CI-00-11-009 Recommendation 21	OPEN: Rolled-forward as Report 4A-CI-00-13-021Recommendation 15
17	We recommend that the OPM Information Technology Security and Privacy Handbook be updated to explicitly require contractor-operated systems to be subject to an annual security controls test performed by a government employee or an independent third party. The security controls tests should be documented using OPM's standard templates.	Recommendation new in FY 2012	CLOSED: 2/27/2013
18	We recommend that OPM continue its efforts to eliminate the unnecessary use of SSNs in accordance with OMB Memorandum M-07-16.	Roll-forward from OIG Reports: • 4A-CI-00-08-022 Recommendation 12, • 4A-CI-00-09-031 Recommendation 22, • 4A-CI-00-10-019 Recommendation 39, and • 4A-CI-00-11-009 Recommendation 28	OPEN: Rolled-forward as Report 4A-CI-00-13-021Recommendation 16

Appendix II

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Information
Officer

MEMORANDUM FOR: [redacted]
CHIEF, INFORMATION SYSTEMS AUDIT GROUP

10/16/2013

FROM: CHUCK SIMPSON
ACTING, CHIEF INFORMATION OFFICER

Subject: Response to the Federal Information Security Management Act Audit – FY2013, Report NO. 4**A-CI-00-13-021**

Thank you for the opportunity to comment on the subject report. The results provided in the draft report consist of a number of recommendations. The recommendations are valuable to our program improvement efforts and most of them are generally consistent with our plan. We plan to continue making improvements in our security risk management strategy and the OPM IT security program.

In reviewing the draft report, we noticed that recommendation #8 which covers specialized security training was reissued. Additional information was submitted since the draft report was issued showing a specialized training participation rate of 94%. We asked for consideration in having recommendation #8 removed from the final audit report.

The CIO's responses to the FY-13 Draft FISMA Audit Report are documented below:

Recommendation 1 *(Rolled-Forward from 2010)*
We recommend that OPM implement 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.

CIO Response:
A CIO initiated Memo directing the centralization of the security responsibilities of Designated Security Officers (DSO) in the Office of Chief Information Security Officer (CISO) was issued by the OPM Director on August, 2012 with an effective date of October 1, 2012. The CIO has already hired three Information System Security Officers with professional IT security experience and certifications and recruitment of an additional one is in progress for a total of four. The initial set of systems has been transition to ISSOs for security management and we expect to have all OPM systems under CISO security management once funding for additional professional security staff becomes available.

__Recommendation 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.

CIO Response:

The OPM SDLC is being applied to OPM's major investment projects. In FY14, a plan with timelines will be developed to enforce the SDLC policy for applicable system development projects.

__Recommendation 3 (*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:

We will continue to assess the Risk Executive Function per NIST Special Publication 800-39 and to explore and make suggestions for implementing this function. The risk executive function will have agency wide authority and responsibility for assessing risk across all OPM Program Offices and to advise senior management on risk management strategies.

__Recommendation 4__

We recommend that the OCIO develop and implement a baseline configuration for [redacted]

CIO Response:

We are working to standardize operating systems and applications throughout the environment. Over the past year, all Windows and Linux operating systems, as well as Microsoft SQL have been given approved baseline images. We will continue to improve our processes and develop and implement configuration baselines for [redacted]

__Recommendation 5__

We recommend that the OCIO conduct routine compliance audits on [redacted] with the OPM baseline configuration once they have been reviewed, updated, and approved.

CIO Response:

We concur with this recommendation and will implement the recommendation on the approved baseline configuration.

__Recommendation 6 (*Rolled-Forward from 2011*)__

We recommend that the OCIO document "accepted" weaknesses identified in Vulnerability scans.

CIO Response:

We concur with this recommendation and will implement the recommendation in FY-14.

Recommendation 7

We recommend that the OCIO establish a centralized network security operations center with the ability to monitor security events for all major OPM systems.

CIO Response:

A centralized monitoring center is established with first level alerting and monitoring for the servers, and network appliances within the major OPM sites. Work has begun on incorporating application and database monitoring and compliance. We will continue to evaluate and look at cost effective ways to implement this recommendation.

Recommendation 8 *(Rolled-Forward from 2010)*

We continue to 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:

We have successfully implemented this recommendation and significant improvements were achieved this year with a completion rate of over 94 percent. Additional information was submitted after the draft report was published that reflects the most current data.

Recommendation 9

We recommend that the OCIO and system owners develop formal corrective action plans to immediately remediate all POA&M weaknesses that are over 120 days overdue.

CIO Response:

The CIO dedicated resources to this task and has successfully closed a majority of POA&Ms that are over 120 days old and will continue to work with program offices to reduce or close those that are outstanding and to develop formal Corrective Action Plans. Most POA&Ms that are over 120 days have dependencies such as funding that is not available or coordination issues with external entities who often are not ready to implement the required changes. It is suggested that the word "immediate" be removed from recommendation 9 since immediate resolution is not feasible.

Recommendation 10

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

CIO Response:

This recommendation has been largely implemented for program offices with open POA&Ms. We will continue to work with program offices to ensure that the "resources required" for POA&Ms are identified and documented.

Recommendation 11

We recommend that system owners submit a POA&M to the OCIO for every system on a quarterly basis.

CIO Response:

This recommendation has been implemented and program offices with open POA&Ms have been updating their POA&Ms in the Trusted Agent system on at least a quarterly basis. High system updates are performed monthly. The POA&M management process has been automated and we no longer require submissions, instead program offices update their POA&Ms in the Trusted Agent Systems under oversight and guidance from the CISO. Program offices that do not have open POA&Ms are not required to perform POA&M updates. Please let us know if you wish to have a discussion on the POA&M automation process.

Recommendation 12(Rolled-Forward from 2012)

We recommend the OCIO configure the VPN servers to [redacted]

CIO Response:

All technological controls are in place and we believe there is a flaw in a vendor's design that will require an out of band patch to repair. We have narrowed the problem to a fault within the UDP connection to the client and we are working with the vendor, Cisco Systems to get this resolved.

Recommendation 13 (Rolled-Forward 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:

We have developed and are in the process of implementing plans for multi-factor PIV authentication for compliance with OMB M-11-11. A major segment of the users on our network infrastructure are using PIV authentication. In FY-14 we will continue to work with program offices to implement PIV authentication for major systems.

Recommendation 14

We recommend that the OCIO expand its continuous monitoring program to include quarterly submissions for High impact systems, more frequent controls testing for all systems, and further implementation of automated tools as outlined in the Information Security Continuous Monitoring Roadmap.

CIO Response:

We have made significant progress implementing Continuous Monitoring at OPM and will continue to expand the program over a 2 year period into FY-15 subject to availability of funds. We plan to implement this specific set of recommendations from the draft report.

Recommendation 15 (Rolled forward from 2008)

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

CIO Response:

We continue to make progress with security controls testing in FY-2013 and expect to have test plans and results for all systems in FY-2014. Security controls testing will be a major part of our continuous monitoring program that is currently being implemented.

Recommendation 16 (*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 eight systems that were not subject to adequate testing in FY 2013.

CIO Response:

We will continue making progress working with program offices on contingency plan testing in FY-14. Due to the current shortage of funding for all ISSOs, the CISO must still rely on decentralized DSOs for support to complete the testing. This has caused delays in implementation and coordination. We ask that the wording in this recommendation be changed from requesting Contingency Plans to be "immediately tested" to tested as soon as possible.

Recommendation 17 (rolled forward from 2011)

We recommend that the OCIO implement and document a centralized (agency-wide) approach to contingency plan testing.

CIO Response:

We will continue efforts to centralize contingency plan testing in FY-14 with the goal of implementing this recommendation.

Recommendation 18 (*Rolled-Forward from 2008*)

We recommend that OPM continue its efforts to eliminate the unnecessary use of SSNs in accordance with OMB Memorandum M-07-16.

CIO Response:

Significant work was done to eliminate the unnecessary use of social security numbers (SSN) including development of a consolidated Action Plan and eliminating them from USAJOBS and the PMF systems. In FY-14, the Privacy Officer will update the action plan and schedule a pilot project with Retirement Services to review business processes to determine how SSNs usage can be reduced. Note that this recommendation requires funding for agency-wide implementation.

Appendix III

Inspector General

Section Report

2013

Annual FISMA Report

Office of Personnel Management

Section 1: Continuous Monitoring Management

1.1 Has the organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems 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

Comments: The OCIO developed a concept of operations document and a continuous monitoring program implementation “roadmap” that describes the stages and timeline for implementing a full continuous monitoring program at OPM. While the initial stages of implementation began in FY 2012, full implementation of the plan is not scheduled to be completed until FY 2015.

1.1.1 Documented policies and procedures for continuous monitoring (NIST SP 800-53: CA-7).

Yes

1.1.2 Documented strategy and plans for continuous monitoring (NIST SP 800-37 Rev 1, Appendix G).

Yes

1.1.3 Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST SP 800-53, NIST 800-53A).

No

Comments: OPM policy requires all owners of OPM-operated systems to submit evidence of continuous monitoring activities at least semiannually, and owners of contractor-operated systems to submit evidence of security control testing annually. Between contractor and agency-operated information systems, only 34 out of 47 systems were subject to adequate security controls testing in FY 2013.

1.1.4 Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as a common and consistent POA&M program that is updated with the frequency defined in the strategy and/or plans (NIST SP 800-53, 800-53A).

Yes

1.2 Please provide any additional information on the effectiveness of the organization’s Continuous Monitoring Management Program that was not noted in the questions above.

No Current Entries

Comments: It has been over six years since all OPM systems were subject to an adequate annual security controls test. OPM’s decentralized approach to IT security has traditionally placed responsibility on the various program offices to test the security controls of their systems. We are optimistic that the quality and consistency of security controls tests will improve with the full implementation of the OCIO’s centralized security structure and with the shift to semi-annual continuous monitoring submissions.

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?**

Yes

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

Yes

2.1.2 **Defined standard baseline configurations.**

Yes

Comments: In FY 2013, OPM put forth significant effort to document and implement new baseline configurations for critical applications, servers, and workstations. At the end of the fiscal year, the OCIO had established baselines and/or build sheets for most major operating platforms used at the agency. However, the baselines for [redacted] are still under development.

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

Yes

Comments: The OCIO uses automated scanning tools to conduct routine compliance audits on the majority of operating platforms used in OPM's server environment. In FY 2013, the OCIO implemented a process to routinely scan [redacted] However, these scans are not performed using an approved [redacted] baseline because, as mentioned in 2.1.2, current baseline configurations for these platforms are in development.

2.1.4 **Process for timely, as specified in organization policy or standards, remediation of scan result deviations.**

Yes

Comments: OPM's Network Management Group (NMG) performs monthly vulnerability scans of all servers using automated scanning tools. NMG has documented accepted weaknesses for OPM user workstations; however, it has not fully documented weaknesses for servers or databases (i.e., vulnerability scan findings that are justified by a business need.)

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

Yes

Section 2: Configuration Management

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

Yes

2.1.7 Process for timely and secure installation of software patches.

Yes

2.1.8 Software assessing (scanning) capabilities are fully implemented (NIST SP 800-53: RA-5, SI-2).

Yes

2.1.9 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)

Yes

2.1.10 Patch management process is fully developed, as specified in organization policy or standards. (NIST SP 800-53: CM-3, SI-2).

Yes

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.

No Current Entries

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 (NIST SP 800-53, AC-2).

Yes

3.1.3 Identifies when special access requirements (e.g., multi-factor authentication) are necessary.

Yes

3.1.4 **If multi-factor authentication is in use, it is linked to the organization's PIV program where appropriate (NIST SP 800-53, IA-2).**

No

Comments: See note in 3.1.5.

3.1.5 **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).**

No

Comments: In FY 2012, the OCIO began an initiative to require PIV authentication to access the agency’s network. As of the end of FY 2013, 30 percent of OPM workstations require PIV authentication for access to the OPM network. However, none of the agency’s 47 major applications require PIV authentication.

3.1.6 **Organization has adequately 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

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

Yes

3.1.8 **Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users (For example: IP phones, faxes, printers are examples of devices attached to the network that are distinguishable from desktops, laptops or servers that have user accounts).**

Yes

3.1.9 **Identifies all user and non-user accounts. (Refers to user accounts that are on a system. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes. They are not associated with a single user or a specific group of users.)**

Yes

3.1.10 **Ensures that accounts are terminated or deactivated once access is no longer required.**

Yes

3.1.11 **Identifies and controls use of shared accounts.**

Yes

Section 3: Identity and Access Management

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.**

No Current Entries

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, and OMB M-07-16, M-06-19).**

Yes

4.1.4 **When applicable, reports to law enforcement within established timeframes (NIST SP 800-61).**

Yes

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, and OMB M-07-16, M-06-19).**

Yes

4.1.6 **Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.**

Yes

Comments: OPM has incident response policies and procedures that govern all systems, including those that reside in a cloud. However, OPM's master system inventory does not document which systems reside in a cloud.

Section 4: Incident Response and Reporting

4.1.7 **Is capable of correlating incidents.**

No

Comments: OPM owns a software product with the technical ability to compare and correlate security incidents over time. However, the correlation features of these tools are not being fully utilized at this time. This tool receives event data from approximately 80 percent of all major OPM systems. Furthermore, OPM does not have a consistent and unified process to monitor and analyze all security incidents. Some incidents cannot be fully investigated due to inconsistent logging practices across systems, and inefficiencies created by program offices running separate monitoring tools on their systems.

4.1.8 **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.**

No Current Entries

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 Risk Executive Function comprised of several IT security professionals. However, as of the end of FY 2012, the 12 primary elements of the Risk Executive Function as described in NIST SP 800-39 were 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, and communicating the agency-wide risks down to the system owners. Although the OCIO improved in assessing risk at the individual system level (see Security Assessment and Authorization section II, above), the OCIO was not fully managing risk at an organization-wide level. As of FY 2013, no further changes have been implemented to address organization-wide risk.

5.1.1 **Documented policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process.**

Yes

For Official Use Only

Section 5: Risk Management

5.1.2 **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: See comment in 5.1.

5.1.3 **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.**

Yes

5.1.4 **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.**

Yes

5.1.5 **Has an up-to-date system inventory.**

Yes

5.1.6 **Categorizes information systems in accordance with government policies.**

Yes

5.1.7 **Selects an appropriately tailored set of baseline security controls.**

Yes

5.1.8 **Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation.**

Yes

5.1.9 **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: The information security controls were adequately assessed for only 34 of OPM's 47 major systems in FY 2013.

5.1.10 **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.**

Yes

Section 5: Risk Management

5.1.11 **Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.**

No

Comments: OPM's continuous monitoring program is not scheduled for full implementation until FY 2015.

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

Yes

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

Yes

5.1.14 **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

5.1.15 **Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies. (NIST SP 800-18, 800-37).**

Yes

5.1.16 **Security authorization package contains accreditation boundaries, defined in accordance with government policies, for organization information systems.**

Yes

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.**

No Current Entries

Section 6: Security Training

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

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.

Yes

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.

No Current Entries

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

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

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.**

No

Comments: See comments in 7.1.4.

7.1.4 **Establishes and adheres to milestone remediation dates.**

No

Comments: Our review indicated that many system owners are not meeting the self-imposed remediation deadlines listed on the POA&Ms. Of OPM's 47 major systems, 22 have POA&M items that are greater than 120 days overdue. We believe that this indicates that POA&M remediation plans are not effective for correcting weaknesses.

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

No

Comments: We interviewed the system owners of five OPM systems with overdue POA&M items. Each owner stated that although they have identified the resources required to address the POA&M items, these resources are not currently available.

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).**

Yes

7.1.7 **Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25).**

No

Comments: We noted that the owners of 10 out of OPM's 47 systems have not identified the resources needed to address POA&M weaknesses, as required by OPM's POA&M policy.

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

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, Rev. 3, Control 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.

No Current Entries

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 If applicable, multi-factor authentication is required for remote access (NIST SP 800-46, Section 2.2, Section 3.3).

Yes

8.1.6 Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.

Yes

Section 8: Remote Access Management

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

Yes

8.1.8 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 connections via VPN [redacted].

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

Yes

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

Yes

8.1.11 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.

No Current Entries

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

Yes

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?

No

Comments: It has been over five years since OPM has adequately tested the contingency plans of all of its major information systems within one fiscal year (see 9.1.4.) In addition, two of OPM's major general support systems were not subject to adequate disaster recovery testing in FY 2013. We believe that this indicates that OPM does not have a FISMA-compliant enterprise-wide business continuity / disaster recovery program.

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 (BIA) into the analysis and strategy development efforts for the organization's Continuity of Operations Plan (COOP), Business Continuity Plan (BCP), and Disaster Recovery Plan (DRP) (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 40 of 47 systems in FY 2013. Of the contingency plan tests we did receive, we continue to notice inconsistency in the quality of the documentation produced for various OPM systems.

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.**

No

Comments: Many OPM systems reside on one of the agency's general support systems. However, two of these general support systems were not adequately tested in FY 2013. In the FY 2011 FISMA audit report we recommended that the OCIO implement a centralized (agency-wide) approach to contingency plan testing. We were informed that a single synchronized functional test is not feasible due to logistical and resource limitations. However, 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 can be remediated if each general support system is subject to a full functional test each year, even if it must be broken into a series of smaller tests.

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

No

Comments: As mentioned in 9.1.4, seven systems were not subject to contingency plan testing in FY 2013, and therefore no after action report was developed.

9.1.9 **Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

9.1.10 **Alternate processing sites are not subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53).**

Yes

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

Yes

9.1.12 **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.**

No Current Entries

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 organization systems and services residing in the cloud external to the organization? Besides the improvement opportunities that may have been identified by the OIG, does the program includes 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 organization systems and services residing in a public cloud.**

Yes

Section 10: Contractor Systems

10.1.2 **The organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with Federal and organization guidelines (NIST SP 800-53: CA-2).**

No

Comments: OPM policy states that system owners must ensure that an annual security controls test is performed for contractor-operated systems by a government employee or an independent third party at the site where contracted information technology services are rendered. However, only 14 of 21 contractor operated systems were adequately tested in FY 2013.

10.1.3 **A complete inventory of systems operated on the organization's behalf by contractors or other entities, including organization systems and services residing in a public cloud.**

Yes

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

Yes

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.**

Yes

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

Yes

10.1.7 **Systems that are owned or operated by contractors or entities, including organization systems and services residing in a public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.**

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.**

No Current Entries

Section 11: Security Capital Planning

11.1 **Has the organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes?**

Yes

Section 11: Security Capital Planning

11.1.1 **Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process.**

Yes

11.1.2 **Includes information security requirements as part of the capital planning and investment process.**

Yes

11.1.3 **Establishes a discrete line item for information security in organizational programming and documentation (NIST SP 800-53: SA-2).**

Yes

11.1.4 **Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST SP 800-53: PM-3).**

Yes

11.1.5 **Ensures that information security resources are available for expenditure as planned.**

Yes

11.2 **Please provide any additional information on the effectiveness of the organization's Security Capital Planning Program that was not noted in the questions above.**

No Current Entries