



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

Final Audit Report

Federal Information Security Management Act Audit FY 2014

Report Number 4A-CI-00-14-016
November 12, 2014

-- CAUTION --

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

EXECUTIVE SUMMARY

Federal Information Security Management Act Audit – FY 2014

Report No. 4A-CI-00-14-016

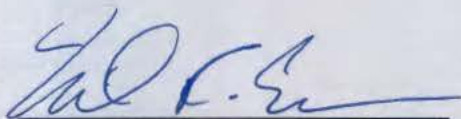
November 12, 2014

Why Did We Conduct the Audit?

Our overall objective was to evaluate OPM's security program and practices, as required by the Federal Information Security Management Act (FISMA). Specifically, we reviewed the status of OPM's information technology security program in accordance with DHS's FISMA Inspector General reporting instructions.

What Did We Audit?

The Office of the Inspector General (OIG) has completed a performance audit of OPM's general FISMA compliance efforts in the specific areas defined in DHS's guidance and the corresponding reporting instructions. Our audit was conducted from April through September 2014 at OPM headquarters in Washington, D.C.



Michael R. Esser
*Assistant Inspector General
for Audits*

What Did We Find?

We determined that the Office of the Chief Information Officer (OCIO) has made some improvements to the U.S. Office of Personnel Management's (OPM) information technology (IT) security program. However, some problem areas that had improved in past years have resurfaced. The following points summarize major improvements or areas of weakness:

- The material weakness related to information security governance has been upgraded to a significant deficiency due to the planned reorganization of the OCIO.
- Eleven major OPM information systems are operating without a valid Authorization. This represents a material weakness in the internal control structure of OPM's IT security program.
- OPM has not fully established a Risk Executive Function.
- The OCIO has implemented an agency-wide information system configuration management policy; however, configuration baselines have not been created for all operating platforms. Also, all operating platforms are not routinely scanned for compliance with configuration baselines.
- OPM does not maintain a comprehensive inventory of servers, databases, and network devices. In addition, we are unable to independently attest that OPM has a mature vulnerability scanning program.
- OPM has established an Enterprise Network Security Operations Center. However, all OPM systems are not adequately monitored.
- Program offices are not adequately incorporating known weaknesses into Plans of Action and Milestones (POA&M) and the majority of systems contain POA&Ms that are over 120 days overdue.
- OPM continues to implement its continuous monitoring plan. However, security controls for all OPM systems are not adequately tested in accordance with OPM policy.
- Not all OPM systems have conducted contingency plan tests in FY 2014.
- Several information security agreements between OPM and contractor-operated information systems have expired.
- Multi-factor authentication is not required to access OPM systems in accordance with OMB memorandum M-11-11.

ABBREVIATIONS

Authorization	Security Assessment and Authorization
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
DSO	Designated Security Officer
ENSOC	Enterprise Network Security Operations Center
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal year
IOC	Internal Oversight and Compliance
ISA	Interconnection Security Agreements
ISSO	Information System Security Officer
IT	Information Technology
ITSP	Information Technology Security and Privacy Group
LAN	Local area network
MOU/A	Memorandum of Understanding/Agreement
NIST	National Institute for Standards and Technology
NMG	Network Management Group
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
POA&M	Plan of Action and Milestones
SDLC	System Development Life Cycle
SIEM	Security information and event management
SO	System Owner
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team
VPN	Virtual private network

TABLE OF CONTENTS

	<u>Page</u>
EXECUTIVE SUMMARY	i
ABBREVIATIONS	ii
I. BACKGROUND	1
II. OBJECTIVES, SCOPE, AND METHODOLOGY	2
III. AUDIT FINDINGS AND RECOMMENDATIONS	5
1. Information Security Governance	5
2. Security Assessment and Authorization	9
3. Risk Management	12
4. Configuration Management	13
5. Incident Response and Reporting	17
6. Security Training	19
7. Plan of Action and Milestones	20
8. Remote Access Management	23
9. Identity and Access Management	24
10. Continuous Monitoring Management	25
11. Contingency Planning	27
12. Contractor Systems	29
13. Security Capital Planning	31
IV. MAJOR CONTRIBUTORS TO THIS REPORT	33
APPENDIX I: Status of Prior OIG Audit Recommendations	
APPENDIX II: The Office of the Chief Information Officer’s October 21, 2014 response to the draft audit report, issued September 18, 2014.	
APPENDIX III: FY 2014 Inspector General FISMA reporting metrics	
REPORT FRAUD, WASTE, AND MISMANAGEMENT	

I. BACKGROUND

On December 17, 2002, the President signed into law the E-Government Act (Public Law 107-347), which includes Title III, the Federal Information Security Management Act (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.

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

FISMA reemphasizes the Chief Information Officer's strategic, agency-wide security responsibility. At OPM, security responsibility is assigned to the agency's Office of the Chief Information Officer (OCIO). FISMA also clearly places responsibility on each agency program office to develop, implement, and maintain a security program that assesses risk and provides adequate security for the operations and assets of programs and systems under its control.

To assist agencies and IGs in fulfilling their FISMA evaluation and reporting responsibilities, the Department of Homeland Security (DHS) Office of Cybersecurity and Communications issued the Fiscal Year (FY) 2014 Inspector General FISMA Reporting Instructions. This document provides a consistent form and format for agencies to report FISMA audit results to DHS. It identifies a series of reporting topics that relate to specific agency responsibilities outlined in FISMA. Our audit and reporting strategies were designed in accordance with the above DHS guidance.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objective

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

- Security Assessment and Authorization;
- 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 five major applications/systems at OPM (see Scope and Methodology for details of these audits), and followed-up on outstanding recommendations from prior FISMA audits (see Appendix I).

Scope and Methodology

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit covered OPM's FISMA compliance efforts throughout FY 2014.

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

audits on the following major information systems:

- Investigations, Tracking, Assigning and Expediting System (Report No. 4A-IS-00-14-017, issued April 3, 2014);
- Services Online System (Report No. 4A-RI-00-14-018, issued April 3, 2014);
- Development Test Production General Support System (Report No. 4A-CI-00-14-015, issued June 6, 2014);
- BENEFEDS and Federal Long Term Care Insurance Program Information Systems (Report No. 4A-RI-00-14-036, issued August 19, 2014); and,
- Dashboard Management Reporting System (Report No. 4A-IS-00-14-064, final audit report not yet issued).

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 2014 Inspector General Federal Information Security Management Act Reporting Instructions;
- OPM Information Technology Security and Privacy Policy Handbook;
- OPM Information Technology Security FISMA Procedures;
- OPM Security Assessment and Authorization Guide;
- OPM Plan of Action and Milestone Standard Operating Procedures;

- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information;
- OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive 12;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- National Institute for Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security;
- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems;
- NIST SP 800-39, Managing Information Security Risk – Organization, Mission, and Information System View;
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems;
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60 Volume 2, Guide for Mapping Types of Information and Information Systems to Security Categories;
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems;
- FIPS Publication 140-2, Security Requirements for Cryptographic Modules; and,
- Other criteria as appropriate.

The audit was performed by the OIG at OPM, as established by the Inspector General Act of 1978, as amended. Our audit was conducted from April through September 2014 in OPM's Washington, D.C. office.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether OPM's practices were consistent with applicable standards. While generally compliant, with respect to the items tested, OPM's OCIO and other program offices were not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

The sections below detail the results of our FY 2014 FISMA audit of OPM's IT Security Program. Many recommendations were issued in prior FISMA audits and are rolled forward from the 2013 FISMA audit (Report No. 4A-CI-00-13-021, issued November 21, 2013).

1. 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. In FY 2013, we also had serious concerns about OPM's ability to govern major system development projects.

In FY 2014, significant changes have been approved related to information security governance. Additional resources were allocated to implement a centralized Information System Security Officer (ISSO) security management structure, and steps were also taken to implement a centralized system development lifecycle (SDLC) methodology. As a result we are upgrading the material weakness to a significant deficiency for FY 2014.

The following sections 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 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 in addition to the responsibilities of their full-time positions.

In FY 2011, the OCIO issued updated IT security and privacy policies, but information security was still managed by DSOs that were generally 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 ISSOs that report to the OCIO. This change was a major milestone in addressing the information security governance material weakness. Through FY 2014, the centralized ISSO structure was

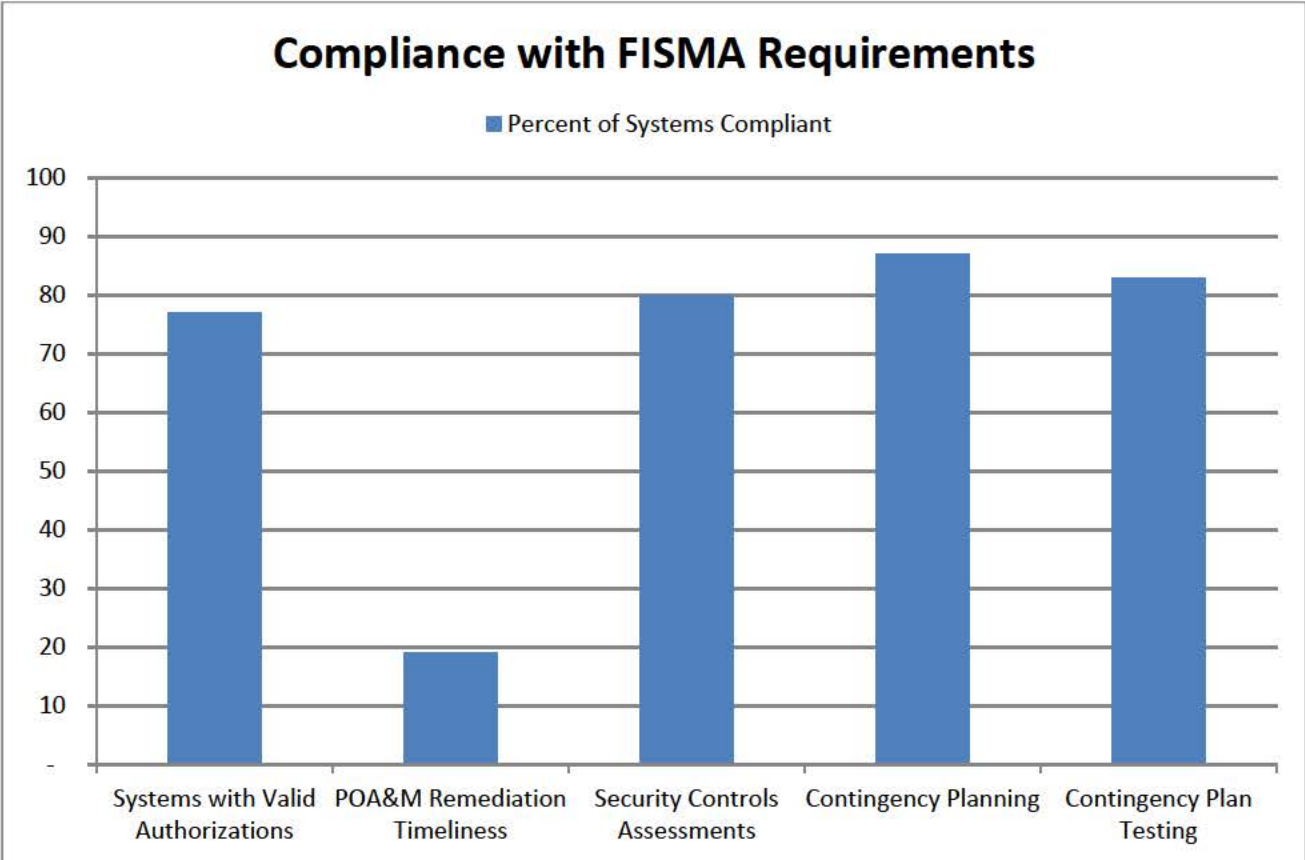
Material weakness related to security governance upgraded to significant deficiency.

partially implemented, with 4 ISSOs assigned security responsibility for 17 of the agency’s information systems.

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 an ISSO.

In FY 2014, OPM’s Director approved a plan to restructure the OCIO that includes funding for 10 additional ISSO positions, bringing the total to 14. After these positions have been filled, the ISSO’s security responsibility will cover 100 percent of OPM information systems.

The findings in this audit report (as highlighted in the chart below) indicate that OPM’s decentralized governance structure continues to result in many instances of non-compliance with FISMA requirements. We believe that these issues could be improved with the full implementation of a centralized security governance structure.



While limited tangible improvements have been made to the security management structure in FY 2014, the ISSO positions that have been planned, approved and funded represent significant improvements over prior years. Therefore, we are upgrading the material weakness to a significant deficiency for FY 2014 due to the imminently planned improvements. However, we will reinstate the material weakness in FY 2015, if the OCIO fails to adequately implement the approved changes.

The audit recommendation related to information security governance will remain open until the planned improvements have been fully implemented.

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 memo directing the centralization of the security responsibilities of Designated Security Officers (DSO) into the Chief Information Security Officer (CISO) organization was issued by the OPM Director on August, 2012 with an effective date of October 1, 2012. The CIO has already hired the first complement of staff with professional IT security experience and certifications, consisting of seven Information Systems Security Officers (ISSO) with an additional four going through the OPM hiring process. The initial set of systems has been transitioned to ISSOs for security management, and we expect to have all OPM systems under ISSO security management in FY15.”

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 2015.

b) Systems development lifecycle methodology

OPM has a history of troubled system development projects. In our opinion, the root causes of these issues have been related to the lack of centralized 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.

At the end of FY 2013, the OCIO published a new SDLC policy, which was a significant first step in implementing a centralized SDLC methodology at OPM. The new SDLC policy incorporated several prior OIG recommendations related to a centralized review process of system development projects. However, policy alone will not improve the historically weak SDLC management capabilities of OPM.

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.

To date, the SDLC is still only applicable to major investment projects, and is not actively enforced for all IT projects in the agency. The OCIO acknowledges the need to enforce the SDLC policy to 100 percent of OPM's IT portfolio, and is currently implementing a reorganization to address this issue by assigning OCIO IT project managers to each of the agency's program offices. However, the staff necessary to properly enforce and oversee the SDLC process for all OPM systems is not in place at this time. In the interim, the OCIO continues to provide training to existing project managers through a Project Management Community of Practice designed to provide guidance on best practices in systems development.

Recommendation 2 (Rolled Forward from FY 2013)

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

OCIO Response:

“The OPM SDLC is being applied to OPM's major investment projects. In FY15, a plan with timelines will be developed to enforce the SDLC policy for all 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 (IOC) 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.

2. 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.)

Our FY 2010 FISMA audit report stated that weaknesses in OPM's Authorization process represented a material weakness in the agency's IT security program. These weaknesses related to incomplete, inconsistent, and poor quality Authorization packages. In FY 2011, the OCIO published updated policies, procedures, and templates designed to improve the overall Authorization process. The OCIO also dedicated resources to oversee OPM program office activity related to system Authorizations. These new controls resulted in a significant improvement in the agency's Authorization packages. The material weakness was lowered to a significant deficiency in FY 2011, and after continued improvement, completely removed as an audit concern in the FY 2012 FISMA report.

The Authorization packages reviewed as part of this FY 2014 audit generally maintained the same satisfactory level of quality that had been observed in recent years. However, of the 21 OPM systems due for Authorization in FY 2014, 11 were not completed on time and are currently operating without a valid Authorization (re-Authorization is required every three years for major information systems). The drastic increase in the number of systems operating without a valid Authorization is alarming, and represents a systemic issue of inadequate planning by OPM program offices to authorize the information systems that they own.

OPM systems operating without an active Authorization represent a material weakness in the internal control structure of the agency's IT security program.

The OCIO's Information Technology Security and Privacy Group (ITSP) continuously provides OPM program offices with adequate guidance and support to facilitate a timely Authorization process. However, many program offices do not initiate the Authorization process early enough to meet its deadlines, do not adequately budget for the contractor support that is needed to complete the process, and/or do not adhere to OPM policies and templates related to the artifacts required for Authorization. Each of these issues contributes to delays in finalizing system Authorizations.

We believe that one of the core causes of these frequent delays is the fact that there are currently no consequences for OPM systems that do not have a valid Authorization to operate. OMB Circular A-130, Appendix III mandates that all Federal information systems have a valid Authorization. We believe that the most effective way to reduce delays is to introduce administrative sanctions for non-compliance with FISMA requirements. We recommend that the performance standards of all OPM major system owners be modified to include a requirement related to FISMA compliance for the systems they own. Furthermore, according to OMB, information systems should not be operating in a production environment without an Authorization. We therefore also recommend that OPM consider shutting down systems that do not have a current and valid Authorization.

We acknowledge that OMB now allows agencies to make ongoing Authorization decisions for information systems based on the continuous monitoring of security controls – rather than enforcing a static, three-year re-Authorization process. However, as discussed in section 10, below, OPM has not yet developed a mature continuous monitoring program. Until such a program is in place, we continue to expect OPM to re-authorize all of its information systems every three years.

The following program offices own one or more systems currently operating without a valid Authorization:

- Office of the Chief Information Officer (five systems);
- Federal Investigative Services (two systems);
- Human Resources Solutions (two systems);
- Office of the Inspector General (one system); and,
- Office of the Chief Financial Officer (one system).

Not only is a large volume (11 out of 47 systems; 23 percent) of OPM's systems operating without a valid Authorization, but several of these systems are amongst the most critical and sensitive applications owned by the agency.

Two of the OCIO systems without an Authorization are general support systems that host a variety of other major applications. Over 65 percent of all systems operated by OPM (not including contractor operated systems) reside on one of these two support systems, and are therefore subject to any security risks that exist on the support systems. Furthermore, two additional systems without Authorizations are owned by OPM's Federal Investigative Services, which is responsible for facilitating background investigations for suitability and security clearance determinations. Any weaknesses in the information systems supporting this program office could potentially have national security implications.

Maintaining active Authorizations for all information systems is a critical element of a Federal information security program, and failure to thoroughly assess and address a system's security weaknesses increases the risk of a security breach. We believe that the volume and sensitivity of OPM systems that are operating without an active Authorization represents a material weakness in the internal control structure of the agency's IT security program.

Recommendation 3

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

OCIO Response:

“As part of the FY15 CIO reorganization, IT Program Managers will work with ISSOs to plan for Security Authorization of systems before existing ATOs expire. However, ATO extensions may be required in a limited number of situations such as the rebuilding of OPM's network where we would need to maintain the existing system and initiate Authorization work after the new design is completed and the rebuilding is underway. We agree that it is important to maintain up-to-date and valid ATOs for all systems but do not believe that this condition rises to the level of a Material Weakness.”

OIG Reply:

The Authorization process is intended to be a comprehensive assessment of the security controls of a major information system, and is a critical step toward preventing security breaches and data loss. Considering the well-publicized data breaches that occurred at OPM in FY 2014, we believe that this is an extremely critical and time sensitive issue. We continue to classify weaknesses in the Authorization process as a material weakness to ensure that the necessary attention and resources are dedicated to this issue.

Recommendation 4

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

OCIO Response:

This recommendation was added after the draft report was issued; the OCIO has not yet had the opportunity to respond.

Recommendation 5

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

OCIO Response:

“The IT Program Managers will work with ISSOs to ensure that OPM systems maintain current ATOs and that there are no interruptions to OPM’s mission and operations.”

3. Risk Management

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

- Tier 1: Organization (Governance);
- Tier 2: Mission/Business Process (Information and Information Flows); and,
- Tier 3: Information System (Environment of Operation). NIST SP 800-39 “Managing Information Security Risk – Organization, Mission, and Information System View” provides additional details of this three-tiered approach.

a) Agency-wide risk management

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

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

In FY 2011, the OCIO organized a Risk Executive Function comprised of several IT security professionals. However, as of the end of FY 2014, 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.

Recommendation 6 (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:

“In FY14, a number of steps were taken to establish and implement the Risk Executive Function per NIST Special Publication 800-39. A proposed Risk Executive Charter and Risk Registry Template were developed and discussed with the Chief Operating Officer who has agreed to serve as the OPM Risk Executive. Additional discussions will be held with the Chief Operating Officer on implementation plans and 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 Authorization process. In addition, OPM policy requires each major information system to be subject to routine security controls testing through a continuous monitoring program (see Continuous Monitoring section 10).

4. Configuration Management

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

a) Agency-wide security configuration policy

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

b) Configuration baselines

In FY 2014, OPM has continued its efforts toward formalizing 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:

- [REDACTED]
- [REDACTED]
- [REDACTED]; and,
- [REDACTED]

However, several additional operating platforms in OPM's network environment do not have baseline configurations documented including, but not limited to, [REDACTED], and [REDACTED]. NIST SP 800-53 Revision 4, 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 7

We recommend that the OCIO develop and implement a baseline configuration for all operating platforms in use by OPM including, but not limited to, [REDACTED] and [REDACTED].

OCIO Response:

“We are working to standardize operating systems and applications throughout the OPM environment. Over the past year, we have established approved baselines for all [REDACTED] [REDACTED] operating systems, as well as [REDACTED]. We will continue to improve our processes and develop and implement configuration baselines for all operating platforms in use by OPM.”

c) United States Government Computer Baseline Configuration

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

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

d) Compliance with baselines

The OCIO uses automated scanning tools to conduct routine compliance audits on 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. However, as mentioned above, there are several operating platforms used by OPM that do not have documented and approved baselines. Without approved baseline configurations these systems cannot be subject to an adequate compliance audit.

NIST SP 800-53 Revision 4, control CM-3, requires agencies to audit activities associated with information system configurations.

Recommendation 8

We recommend the OCIO conduct routine compliance scans against established baseline configurations for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 6 has been completed.

OCIO Response:

“We expand our routine compliance scans as we implement additional configuration baselines for additional operating platforms.”

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, track, and document change requests.

OPM also has a software product that has the capability to detect, approve, and revert all changes made to information systems. However, this capability has not been fully implemented, and OPM cannot ensure that all changes made to information systems have been properly documented and approved.

OPM’s Information Security and Privacy Policy Handbook states that “SOs shall ensure the information system employs automated mechanisms to. . . Inhibit change until designated approvals are received.”

Recommendation 9

We recommend the OCIO implement technical controls that prevent configuration changes without proper documentation and approvals.

OCIO Response:

“Configuration changes require approval by the Change Control Board which meets on a regular basis. However, there are emergency situations where changes might be made outside of the CCB cycle. We will ensure required documentation and approvals are in place for all configuration changes.”

OIG Reply:

While emergency changes may be required outside of the CCB cycle, we still recommend that automated mechanisms be implemented to prevent changes to information systems

without proper approval. Emergency changes should still require approval even if the documentation occurs after the change has been implemented.

f) Vulnerability scanning

We were told in an interview that OPM's Network Management Group (NMG) performs monthly vulnerability scans using automated scanning tools. However, we have been unable to obtain tangible evidence that vulnerability scans have been routinely conducted for all OPM servers in FY 2014. As a result, we are unable to independently attest that OPM has a mature vulnerability scanning program, and must indicate as such on the FISMA metrics provided to OMB.

The OIG is unable to independently verify that OPM has a mature vulnerability scanning program.

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 2014.

We also determined through interviews and our independent vulnerability scanning process that OPM does not maintain an accurate centralized inventory containing all servers and databases that reside within the network.

NIST SP 800-53 Revision 4, control PM-5, requires agencies to develop and maintain an inventory of its information systems.

Recommendation 10

We recommend that the OCIO develop and maintain a comprehensive inventory of all servers, databases, and network devices that reside on the OPM network.

OCIO Response:

“Our Asset Management System serves as a repository for servers, databases and network devices. We will continue to work to identify and document all assets residing on the OPM network.”

Recommendation 11

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

OCIO Response:

“We will continue to improve our scanning capabilities to ensure that vulnerability scanning is conducted on all network devices documented in our inventory.”

Recommendation 12

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

OCIO Response:

“We concur with this recommendation and will implement the recommendation in FY15.”

Recommendation 13 (Rolled Forward from 2011)

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

OCIO Response:

“We concur with this recommendation and will implement the recommendation in FY15.”

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. The OCIO also utilizes a third party patching software management program to manage and maintain all non-operating system software. However, through our independent vulnerability scans on a sample of servers we determined that numerous servers are not timely patched.

Recommendation 14

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

OCIO Response:

The OCIO did not respond to this recommendation.

5. Incident Response and Reporting

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

a) Identifying and reporting incidents internally

OPM's Incident Response and Reporting Guide requires any user of the agency's IT resources to immediately notify OPM's Situation Room when IT security incidents occur. OPM reiterates 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 several different software tools to prevent and detect intrusions and malware in the agency's network.

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 security information and event management (SIEM) tool with the technical ability to automatically detect, analyze, and correlate potential security incidents over time. However, the correlation features of this tool are not fully utilized at this time. This tool only receives event data from approximately 80 percent of major OPM information systems.

In FY 2014, the OCIO established an Enterprise Network Security Operations Center (ENSOC) that provides continuous centralized support for OPM's security incident prevention/management program. However, the ENSOC cannot adequately fulfill its purpose if it does not receive data from all OPM systems.

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

Recommendation 15

We recommend that the OCIO expand the capabilities of the ENSOC to ensure that security incidents from all OPM-operated information systems are centrally analyzed and correlated.

OCIO Response:

“A centralized monitoring center was put in place with first level alerting and monitoring for the servers and network appliances within the major OPM sites. We are expanding our monitoring capabilities to cover OPM operated information systems wherever feasible.”

d) Responding to incidents

As mentioned above, OPM owns a tool with the ability to automatically detect and report potential security incidents by analyzing data from various sources. After analyzing the data, the tool alerts security analysts to potential security incidents.

However, the tool needs to be configured to collect relevant and meaningful data so the potential security alerts contain fewer false-positives. The OPM systems currently providing data to the SIEM are over-reporting log and event data, which results in an excessive amount of data for security analysts to review. The number of alerts that security analysts must review and identify as false-positive creates a backlog that could cause a delay in identifying and responding to actual incidents. This issue is compounded by the fact that the SIEM is not receiving any data from approximately 20 percent of OPM systems.

Recommendation 16

We recommend that OCIO configure its security information and event management tool to collect and report meaningful data, while reducing the volume of non-sensitive log and event data.

OCIO Response:

“The security event management system collects important data that we use to access threats to the OPM environment. We will continue to refine our configuration settings to improve the quality of the data being reviewed.”

6. 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

OPM maintains an adequate IT security training program.

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 99 percent of OPM's employees and contractors completed the security awareness training course in FY 2014.

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, 95 percent have completed specialized IT training in FY 2014.

7. 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

In November 2013, the OIG issued the FY 2013 FISMA audit report with 16 audit recommendations. We verified that all 16 recommendations were appropriately incorporated into the OCIO's master POA&M.

However, all known security weaknesses were appropriately incorporated to the system-specific POA&Ms for only 29 of OPM's 47 systems. This includes 14 of the 25 systems operated by OPM, and 15 of the 22 systems operated by a contractor.

Failure to incorporate all known IT security weaknesses into the associated POA&M limits the agency's ability to effectively identify, assess, prioritize, and monitor the progress of the corrective efforts to remediate identified weaknesses. The following program offices failed to submit adequate documentation for one or more systems that they own:

- Human Resources Solutions (four systems);
- Federal Investigative Services (three systems);
- Office of the Inspector General (three systems);
- Healthcare and Insurance (three systems);

- Office of the Chief Information Officer (two systems);
- Office of the Chief Financial Officer (one system);
- Retirement Services (one system); and,
- Employee Services (one system).

Recommendation 17

We recommend that the OCIO and program offices that own information systems ensure that all known security weaknesses are incorporated into the appropriate POA&M.

OCIO Response:

“A centralized automated POA&M management system is in place and staffed by a dedicated resource to ensure that all findings, recommendations and POA&Ms are managed to resolution and we believe that this process is working as intended. Additional information was submitted to substantiate elimination of this recommendation.”

OIG Reply:

While evidence was provided in response to the draft audit report to indicate that all findings from the FY 2013 FISMA audit report were included in a POA&M, the program offices listed above have not adequately incorporated all known IT security weaknesses into the associated POA&M. We continue to recommend that the OCIO and program offices that own information systems ensure that all known security weaknesses are incorporated into the appropriate POA&M.

b) Prioritize weaknesses

OPM’s POA&M Guide requires each program office 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. Out of OPM’s 47 operational systems, 38 have POA&M items that are greater than 120 days overdue. We issued an audit recommendation in FY 2012 related to overdue POA&M items, and because overdue POA&Ms continue to be an issue, we will roll forward this recommendation into FY 2014.

Recommendation 18 (Rolled forward from FY 2012)

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 most POA&Ms that are over 120 days overdue and will continue to develop formal Action Plans for those remaining weaknesses. Most POA&Ms that are over 120 days overdue have dependencies that need to be coordinated with external entities that often are not ready to implement the required changes.”

OIG Reply:

Evidence was provided in response to the draft audit report to indicate that corrective action plans have been created for 25 of the 38 systems with POA&M items over 120 overdue. As part of the audit resolution process, the OCIO should provide IOC with evidence that the program offices for the remaining 13 systems have created corrective action plans.

d) Identifying resources to remediate weaknesses

POA&Ms for 9 of the 47 OPM systems did not identify the resources needed to address POA&M weaknesses in FY 2014, as required by OPM’s POA&M policy. We made this recommendation in the FY 2013 FISMA audit report, and closed it in early FY 2014 based on evidence provided by the OCIO which indicated that POA&Ms had been updated. However, the fieldwork for this audit indicates that this situation continues to be a problem.

Recommendation 19

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

OCIO Response:

“This recommendation has been implemented for most open POA&Ms. We will continue to ensure that the ‘resources required’ for POA&Ms are identified and documented.”

OIG Reply:

Evidence was provided in response to the draft audit report to indicate that required resources have been identified and documented for outstanding POA&M items; no further action is required.

e) OCIO tracking and reviewing POA&M activities

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 review the documentation to determine whether or not the evidence provided was appropriate.

We selected one closed POA&M item from 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.

OPM appears to maintain adequate proof-of-closure documentation when closing POA&M weaknesses.

8. 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. OIG has reviewed the VPN access list to ensure that there are no shared accounts and that each user account has been tied to an individual. The agency maintains logs of individuals who remotely access the network, and the logs are reviewed on a monthly basis for unusual activity or trends.

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

In previous years, we discovered that remote access sessions do not terminate or lock out after [REDACTED] inactivity as required by FISMA. OPM has acknowledged the issue and stated that the weakness cannot be remediated until the VPN vendor releases a software update.

Recommendation 20 (Rolled-Forward from 2012)

We recommend the OCIO configure the VPN servers to terminate VPN sessions after [REDACTED] of inactivity.

OCIO Response:

“All technological controls are in place. We believe there is a flaw in the vendor’s product that will require a patch update that the vendor so far is unwilling to provide. We will explore an alternative product solution.”

9. 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 Windows and mainframe active user lists against a list of terminated employees from the past year. Nothing came to our attention to indicate that there are weaknesses in OPM’s access termination management process.

c) Multi-factor authentication with PIV

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

OPM not compliant with OMB M-11-11 which mandates the use of PIV credentials for multi-factor authentication for major information systems.

In FY 2012, the OCIO began an initiative to require PIV authentication to access the agency’s network. As of the end of FY 2014, over 95 percent of OPM workstations require PIV authentication to access to the OPM network. However, none of the agency’s 47 major applications require PIV authentication.

Recommendation 21 (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 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 FY15 we will continue to implement PIV authentication for major systems.”

10. 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. The OCIO also creates continuous monitoring plans each fiscal year that clearly describe the type and frequency of NIST SP 800-53 Revision 4 security controls that must be tested throughout the year.

As stated previously in Section 1, the ISSO function has not been fully established at OPM. 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 continuous monitoring strategy document that provides a high-level strategy for the implementation of information security continuous monitoring. While the initial stages of implementation began in FY 2012, full implementation of the plan is an ongoing process. The OCIO achieved the FY 2014 milestones outlined in the roadmap which included quarterly reporting for high impact systems. The next stage in the OCIO’s plan involves requiring continuous monitoring by contractor-operated systems and implementation of the DHS Continuous Diagnostic and Mitigation program.

Recommendation 22

We recommend that the OCIO expand its continuous monitoring program to include mandatory continuous monitoring for contractor-operated systems and implementation of the DHS Continuous Diagnostic and Mitigation program as outlined in the OCIO's continuous monitoring strategy.

OCIO Response:

“In FY15, we will continue to work with DHS to implement the Continuous Diagnostic and Mitigation program at OPM. As a result of working with DHS, OPM has been moved higher (sooner) in the implementation schedule. To date, we have submitted OPM requirements and hosted a Reading Room for vendors to validate our requirements. There will also be a major initiative to expand Continuous Monitoring programs to contractor systems where feasible.”

c) Assessment of individual system security controls

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

We requested the security test results for all OPM-operated systems for April 2014 in order to review them for quality and consistency. We will test the October 2014 submission as part of the FY 2015 FISMA audit. For the April submission, we were only provided adequate testing documentation for 18 out of the 25 major systems operated by OPM. The following program offices failed to submit adequate documentation for one or more systems that they own:

- Office of the Chief Information Officer (four systems);
- Office of the Inspector General (two systems); and,
- Office of the Chief Financial Officer (one system).

At this time, security controls testing for contractor-operated systems is still only required once per year. A review of contractor system security control testing (see section 12, below) indicates that only 19 out of 22 contractor-operated systems were adequately tested in this fiscal year.

Between contractor and agency-operated information systems, only 37 out of 47 systems were subject to adequate security controls testing in FY 2014. 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 eight years since all OPM systems were subject to an adequate 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 continues to contribute 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 23 (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 and expect to have test plans and results for all systems in FY15. Security controls testing is a major part of our continuous monitoring program that is being implemented for OPM systems.”

11. 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 2014.

a) Documenting contingency plans of individual OPM systems

We received updated contingency plans for 41 out of 47 information systems on OPM's master system inventory. We then verified that these contingency plans followed the template developed by the OCIO that is based on the guidance of NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems. The following program offices failed to submit adequate contingency planning documentation for one or more systems that they own:

- Retirement Services (three systems);
- Office of the Chief Information Officer (two systems); and,
- Office of the Inspector General (one system).

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

Recommendation 24

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

OCIO Response:

“We will continue making progress on contingency plan updates in FY15. Having additional ISSOs onboard is expected to significantly improve our ability to accomplish this task.”

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 39 of 47 systems in FY 2014. This is a slight decrease from the number of systems that were tested in FY 2013. The following program offices failed to submit adequate documentation for one or more systems that they own:

- Office of the Chief Information Officer (five systems);
- Employee Services (one system);
- Healthcare and Insurance (one system); and,
- Office of the Inspector General (one system).

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

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

Recommendation 25 (Rolled-Forward from 2008)

We recommend that OPM's program offices test the contingency plans for each system on an annual basis. The contingency plans should be immediately tested for the eight systems that were not subject to adequate testing in FY 2014.

OCIO Response:

“We will continue making progress on contingency plan testing in FY15. Having additional ISSOs onboard is expected to significantly improve our ability to accomplish this task.”

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 full functional test was performed in FY 2014. Also, another one of OPM’s major general support system, the LAN/WAN general support system, was not subject to a full functional disaster recovery test.

NIST SP 800-53 Revision 4, control CP-4, states that owners of FIPS 199 “high” systems should test “the contingency plan at the alternate processing site.” 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 26 (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 making progress on contingency plan testing in FY15. Having additional ISSOs onboard is expected to significantly improve our ability to accomplish this task.”

12. 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.

a) Contractor system documentation

OPM's master system inventory indicates that 22 of the agency's 47 major applications are operated by a contractor. However, the master system inventory does not indicate if the system is hosted in a cloud environment. NIST 800-53 Revision 4 states that the agency must develop and maintain an inventory of its information systems. The FY 2014 FISMA Reporting Metrics indicate that a complete inventory of systems indicates which systems and services reside in a public cloud environment.

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

While the OCIO tracks ISAs, it does not track Memorandums of Understanding/Agreement (MOU/A). These documents outline the terms and conditions for sharing data and information resources in a secure manner. We were told that program offices were responsible for maintaining MOU/As. While we have no issue with the program offices maintaining the memorandums, the OCIO should track MOU/As to ensure that valid agreements are in place for each documented ISA.

Recommendation 27

We recommend that the OCIO identify agency systems that reside in a public cloud and document those systems on the master system inventory.

OCIO Response:

“This recommendation was addressed and documented on the master system inventory.”

OIG Reply:

Evidence was provided in response to the draft audit report to indicate that the OCIO has identified systems that reside in a public cloud; no further action is required.

Recommendation 28

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

OCIO Response:

“We will continue to improve ISA processes to ensure that they are maintained in a valid and consistent manner. Having additional ISSOs onboard is expected to significantly improve our ability to accomplish this task.”

Recommendation 29

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

OCIO Response:

“We will continue to improve MOU processes to ensure they are maintained in a valid and consistent manner. Having additional ISSOs onboard is expected to significantly improve our ability to accomplish this task.”

b) 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. We were only provided testing documentation for 19 out of the 22 systems. In the tests we received, we noticed significant differences in quality and consistency. We would normally make a recommendation for the OCIO to take action to improve the quality and consistency of these security control tests. However, the OCIO’s continuous monitoring strategy includes requiring continuous monitoring for contractor-operated systems. The OCIO also maintains a continuous monitoring plan that describes the type and frequency of NIST SP 800-53 Revision 4 security controls that must be tested throughout the year. We believe that use of the continuous monitoring plan will improve the quality and consistency of contractor system security control tests. See section 10 above for the related recommendation.

13. Security Capital Planning

NIST SP 800-53 Revision 4, control SA-2, 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.

As mentioned previously in Section 2, the drastic increase in the number of systems operating without a valid Authorization is alarming, and represents a systemic issue of inadequate planning by OPM program offices to authorize the information systems that they own. Please see section 2 for audit recommendations related to this issue.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[REDACTED], Auditor-In-Charge

[REDACTED], Lead IT Auditor

[REDACTED], IT Auditor

[REDACTED], IT Auditor

[REDACTED], IT Auditor

[REDACTED], IT Auditor

[REDACTED], IT Auditor

[REDACTED] Group Chief

Status of Prior OIG Audit Recommendations

The tables below outline the current status of prior audit recommendations issued in FY 2013 by the Office of the Inspector General.

Report No. 4A-CI-00-13-021: FY 2013 Federal Information Security Management Act Audit, issued November 21, 2013

<u>Rec #</u>	<u>Original Recommendation</u>	<u>Recommendation History</u>	<u>Current Status</u>
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: <ul style="list-style-type: none"> • 4A-CI-00-10-019 Recommendation 4, • 4A-CI-00-11-009 Recommendation 2, and • 4A-CI-00-12-016 Recommendation 1 	OPEN: Rolled-forward as Report 4A-CI-00-14-016 Recommendation 1
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.	Recommendation new in FY 2013	OPEN: Rolled-forward as Report 4A-CI-00-14-016 Recommendation 2
3	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: <ul style="list-style-type: none"> • 4A-CI-00-11-009 Recommendation 6 and • 4A-CI-00-12-016 Recommendation 2 	OPEN: Rolled-forward as Report 4A-CI-00-14-016 Recommendation 6
4	We recommend that the OCIO develop and implement a baseline configuration for both ██████████ databases.	Recommendation new in FY 2013	CLOSED 9/16/2014
5	We recommend that the OCIO conduct routine compliance audits on ██████████ databases with the OPM baseline configuration once they have been reviewed, updated, and approved.	Recommendation new in FY 2013	CLOSED 9/16/2014
6	We recommend that the OCIO document “accepted” weaknesses identified in vulnerability scans.	Roll-forward from OIG Reports: <ul style="list-style-type: none"> • 4A-CI-00-11-009 Recommendation 9 and • 4A-CI-00-12-016 Recommendation 4 	OPEN: Rolled-forward as Report 4A-CI-00-14-016 Recommendation 13

Appendix I

Status of Prior OIG Audit Recommendations

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.	Roll-forward from OIG Reports: • 4A-CI-00-12-016 Recommendation 6	CLOSED 11/25/2013
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.	Roll-forward from OIG Reports: • 4A-CI-00-12-016 Recommendation 8	OPEN: Rolled-forward as Report 4A-CI-00-14-016 Recommendation 18
9	We recommend that all POA&Ms list the specific resources required to address each security weakness identified.	Roll-forward from OIG Reports: • 4A-CI-00-12-016 Recommendation 9	CLOSED 11/25/2013
10	We recommend the OCIO configure the VPN servers to terminate VPN sessions after [REDACTED] of inactivity.	Roll-forward from OIG Reports: • 4A-CI-00-12-016 Recommendation 10	OPEN: Rolled-forward as Report 4A-CI-00-14-016 Recommendation 20
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.	Roll-forward from OIG Reports: • 4A-CI-00-12-016 Recommendation 11	OPEN: Rolled-forward as Report 4A-CI-00-14-016 Recommendation 21
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.	Recommendation new is FY 2013	CLOSED 9/18/2014
13	We recommend that OPM ensure that an annual test of security controls has been completed for all systems.	Roll-forward from OIG Reports: • 4A-CI-00-08-022 Recommendation 1, • 4A-CI-00-09-031 Recommendation 6, • 4A-CI-00-10-019 Recommendation 10, • 4A-CI-00-11-009 Recommendation 11, and • 4A-CI-00-12-016 Recommendation 14	OPEN: Rolled-forward as Report 4A-CI-00-14-016 Recommendation 23

Status of Prior OIG Audit Recommendations

14	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.	Roll-forward from OIG Reports: <ul style="list-style-type: none"> • 4A-CI-00-08-022 Recommendation 2, • 4A-CI-00-09-031 Recommendation 9, • 4A-CI-00-10-019 Recommendation 30, • 4A-CI-00-11-009 Recommendation 19, and • 4A-CI-00-12-016 Recommendation 15 	OPEN: Rolled-forward as Report 4A-CI-00-14-016 Recommendation 25
15	We recommend that the OCIO implement and document a centralized (agency-wide) approach to contingency plan testing.	Roll-forward from OIG Reports: <ul style="list-style-type: none"> • 4A-CI-00-11-009 Recommendation 21 and • 4A-CI-00-12-016 Recommendation 16 	OPEN: Rolled-forward as Report 4A-CI-00-14-016 Recommendation 26
16	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: <ul style="list-style-type: none"> • 4A-CI-00-08-022 Recommendation 12, • 4A-CI-00-09-031 Recommendation 22, • 4A-CI-00-10-019 Recommendation 39, • 4A-CI-00-11-009 Recommendation 28, and • 4A-CI-00-12-016 Recommendation 18 	CLOSED 9/26/2014

Appendix II



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

Chief Information
Officer

MEMORANDUM FOR [REDACTED]
CHIEF, INFORMATION SYSTEMS AUDIT GROUP

FROM: DONNA K. SEYMOUR
CHIEF INFORMATION OFFICER

Donna K. Seymour
10/24/2014

Subject: Response to the Federal Information Security Management Act Audit
FY2014, Report NO. 4A-CI-00-14-016

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 #15 which covers specialized security training was issued. Additional information was submitted since the draft report was issued showing a specialized training participation rate above 90%. In addition, recommendation #16 states that only 6 of 16 audit findings were incorporated into POA&Ms, and according to our records, all 16 recommendations were documented and converted to POA&Ms and centrally managed. Recommendation #26 is already in place and the information has been provided to your office. We ask for consideration in having recommendations #15, #16 and #26 removed from the final audit report.

The CIO's responses to the FY14 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 Chief Information Security Officer. 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 memo directing the centralization of the security responsibilities of Designated Security Officers (DSO) into the Chief Information Security Officer (CISO) organization was issued by the OPM Director on August, 2012 with an effective date of October 1, 2012. The CIO has already hired the first complement of staff with professional IT security experience and certifications, consisting of seven Information Systems Security Officers (ISSO) with an additional four going through the OPM hiring process. The initial set of systems has been transitioned to ISSOs for security management, and we expect to have all OPM systems under ISSO security management in FY15.

Recommendation #2

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

CIO Response:

The OPM SDLC is being applied to OPM's major investment projects. In FY15, a plan with timelines will be developed to enforce the SDLC policy for all applicable system development projects.

Recommendation #3

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

CIO Response:

As part of the FY15 CIO reorganization, IT Program Managers will work with ISSOs to plan for Security Authorization of systems before existing ATOs expire. However, ATO extensions may be required in a limited number of situations such as the rebuilding of OPM's network where we would need to maintain the existing system and initiate Authorization work after the new design is completed and the rebuilding is underway. We agree that it is important to maintain up-to-date and valid ATOs for all systems but do not believe that this condition rises to the level of a Material Weakness.

Recommendation #4

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

CIO Response:

The IT Program Managers will work with ISSOs to ensure that OPM systems maintain current ATOs and that there are no interruptions to OPM's mission and operations.

Recommendation #5 (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:

In FY14, a number of steps were taken to establish and implement the Risk Executive Function per NIST Special Publication 800-39. A proposed Risk Executive Charter and Risk Registry Template were developed and discussed with the Chief Operating Officer who has agreed to serve as the OPM Risk Executive. Additional discussions will be held with the Chief Operating Officer on implementation plans and strategies.

Recommendation #6

We recommend that the OCIO develop and implement a baseline configuration for all operating platforms in use by OPM including, but not limited to [REDACTED]

CIO Response:

We are working to standardize operating systems and applications throughout the OPM environment. Over the past year, we have established approved baselines for all [REDACTED] operating systems, as well as [REDACTED]. We will continue to improve our processes and develop and implement configuration baselines for all operating platforms in use by OPM.

Recommendation #7

We recommend the OCIO conduct routine compliance scans against established baseline configurations for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 6 has been completed.

CIO Response:

We expand our routine compliance scans as we implement additional configuration baselines for additional operating platforms.

Recommendation #8

We recommend the OCIO implement technical controls that prevent configuration changes without proper documentation and approvals.

CIO Response:

Configuration changes require approval by the Change Control Board which meets on a regular basis. However, there are emergency situations where changes might be made outside of the CCB cycle. We will ensure required documentation and approvals are in place for all configuration changes.

Recommendation #9

We recommend that the OCIO develop and maintain a comprehensive inventory of all servers, databases, and network devices that reside on the OPM network.

CIO Response:

Our Asset Management System serves as a repository for servers, databases and network devices. We will continue to work to identify and document all assets residing on the OPM network.

Recommendation #10

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

CIO Response:

We will continue to improve our scanning capabilities to ensure that vulnerability scanning is conducted on all network devices documented in our inventory.

Recommendation #11

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

CIO Response:

We concur with this recommendation and will implement the recommendation in FY15.

Recommendation #12 (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 FY15.

Recommendation #13

We recommend that the OCIO expand the capabilities of the ENSOC to ensure that security incidents from all OPM-operated information systems are centrally analyzed and correlated.

CIO Response:

A centralized monitoring center was put in place with first level alerting and monitoring for the servers and network appliances within the major OPM sites. We are expanding our monitoring capabilities to cover OPM operated information systems wherever feasible.

Recommendation #14

We recommend that OCIO configure its security information and event management tool to collect and report meaningful data, while reducing the volume of non-sensitive log and event data.

CIO Response:

The security event management system collects important data that we use to access threats to the OPM environment. We will continue to refine our configuration settings to improve the quality of the data being reviewed.

Recommendation #15

We recommend that the OCIO ensure that all employees with significant information security responsibility take meaningful and appropriate specialized security training on an annual basis.

CIO Response:

We have successfully implemented this recommendation and significant improvements were achieved this year with a completion rate of over 90 percent. Additional information was submitted to substantiate elimination of this recommendation.

Recommendation #16

We recommend that the OCIO and program offices that own information systems ensure that all known security weaknesses are incorporated into the appropriate POA&M.

CIO Response:

A centralized automated POA&M management system is in place and staffed by a dedicated resource to ensure that all findings, recommendations and POA&Ms are managed to resolution and we believe that this process is working as intended. Additional information was submitted to substantiate elimination of this recommendation.

Recommendation #17

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 most POA&Ms that are over 120 days overdue and will continue to develop formal Action Plans for those remaining weaknesses. Most POA&Ms that are over 120 days overdue have dependencies that need to be coordinated with external entities that often are not ready to implement the required changes.

Recommendation #18

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

CIO Response:

This recommendation has been implemented for most open POA&Ms. We will continue to ensure that the “resources required” for POA&Ms are identified and documented.

Recommendation #19 (Rolled-Forward from 2012)

We recommend the OCIO configure the VPN servers to terminate VPN sessions after [REDACTED] inactivity.

CIO Response:

All technological controls are in place. We believe there is a flaw in the vendor’s product that will require a patch update that the vendor so far is unwilling to provide. We will explore an alternative product solution.

Recommendation #20 (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 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 FY15 we will continue to implement PIV authentication for major systems.

Recommendation #21

We recommend that the OCIO expand its continuous monitoring program to include mandatory continuous monitoring for contractor-operated systems and implementation of the DHS Continuous Diagnostic and Mitigation program as outlined in continuous monitoring strategy.

CIO Response:

In FY15, we will continue to work with DHS to implement the Continuous Diagnostic and Mitigation program at OPM. As a result of working with DHS, OPM has been moved higher (sooner) in the implementation schedule. To date, we have submitted OPM requirements and hosted a Reading Room for vendors to validate our requirements. There will also be a major initiative to expand Continuous Monitoring programs to contractor systems where feasible.

Recommendation #22 (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 and expect to have test plans and results for all systems in FY15. Security controls testing is a major part of our continuous monitoring program that is being implemented for OPM systems.

Recommendation #23

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

CIO Response:

We will continue making progress on contingency plan updates in FY15. Having additional ISSOs onboard is expected to significantly improve our ability to accomplish this task.

Recommendation #24 (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 2014.

CIO Response:

We will continue to make progress on contingency plan testing in FY15. Having additional ISSOs onboard is expected to significantly improve our ability to accomplish this task.

Recommendation #25 (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 our efforts to centralize contingency plan testing in FY15. Having additional ISSOs onboard is expected to significantly improve our ability to accomplish this task.

Recommendation #26

We recommend that the OCIO identify agency systems that reside in a public cloud and document those systems on the master system inventory.

CIO Response:

This recommendation was addressed and documented on the master system inventory.

Recommendation #27

We recommend that the OCIO ensure that all ISA's are valid and properly maintained.

CIO Response:

We will continue to improve ISA processes to ensure that they are maintained in a valid and consistent manner. Having additional ISSOs onboard is expected to significantly improve our ability to accomplish this task.

Recommendation #28

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

CIO Response:

We will continue to improve MOU processes to ensure they are maintained in a valid and consistent manner. Having additional ISSOs onboard is expected to significantly improve our ability to accomplish this task.

Recommendation #29 (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 elimination of the use of SSNs from USAJOBS and the PMF systems. In FY15, the Privacy Officer will conduct a pilot project with an OPM program office to review business processes to determine how SSN usage can be reduced further.

Inspector General

Section Report

2014

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

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

Yes

1.1.2 Documented strategy for information security continuous monitoring (ISCM).

Yes

1.1.3 Implemented ISCM for information technology assets.

No

Comments:

The Office of the Chief Information Officer (OCIO) developed a continuous monitoring strategy document that provides a high-level strategy for the implementation of information security continuous monitoring. While the initial stages of implementation began in fiscal year (FY) 2012, full implementation of the plan is an ongoing process. The OCIO achieved the FY 2014 milestones outlined in the roadmap which included quarterly reporting for high impact systems. The next stage in the OCIO's plan involves requiring continuous monitoring by contractor operated systems and implementation of the Department of Homeland Security Continuous Diagnostic and Mitigation program.

1.1.4 Evaluate risk assessments used to develop their ISCM strategy.

Yes

1.1.5 Conduct and report on ISCM results in accordance with their ISCM strategy.

Yes

1.1.6 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, 800-53A).

No

Comments:

Only 18 of the 25 systems subject to continuous monitoring were adequately tested in accordance with Office of Personnel Management (OPM) policy.

Section 1: Continuous Monitoring Management

1.1.7 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.

N/A

Section 2: Configuration Management

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

No

Comments:

As noted below, there are notable deficiencies in OPM's configuration management program, and we do not consider this program to be substantially compliant with FISMA requirements, OMB policy, and applicable NIST guidelines.

2.1.1 Documented policies and procedures for configuration management.

Yes

2.1.2 Defined standard baseline configurations.

No

Comments:

In FY 2014, OPM has continued its efforts toward formalizing baseline configurations for critical applications, servers, and workstations. However, several additional operating platforms in OPM's network environment do not have baseline configurations documented including, but not limited to, [REDACTED].

2.1.3 Assessments of compliance with baseline configurations.

No

Comments:

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. However, there are several operating platforms used by OPM that do not have documented and approved baselines. Without approved baseline configurations these systems cannot be subject to an adequate compliance audit.

Section 2: Configuration Management

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

No

Comments: OPM performs monthly vulnerability scans using automated scanning tools. However, we have been unable to obtain tangible evidence that vulnerability scans have been routinely conducted for all OPM servers in FY 2014. As a result, we are unable to independently attest that OPM has a mature vulnerability scanning program.

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

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

No

Comments: OPM also has a software product that has the capability to detect, approve, and revert all changes made to information systems. However, this capability has not been fully implemented, and OPM cannot ensure that all changes made to information systems have been properly documented and approved.

2.1.7 Process for timely and secure installation of software patches.

No

Comments: See comment in 2.1.4

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

No

Comments: See comment in 2.1.4

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)

No

Comments: See comment in 2.1.4

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

No

Comments: See comment in 2.1.4

Section 2: Configuration Management

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

N/A

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

Yes

2.3.1 Is there a process for mitigating the risk introduced by those deviations?

Yes

Section 3: Identity and Access Management

3.1 Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and 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.

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 2014, over 95 percent of OPM workstations require PIV authentication to access to the OPM network. However, none of the agency's 47 major applications require PIV authentication.

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).

Yes

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:

See comment in 3.1.3

Section 3: Identity and Access Management

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, and printers are examples of devices attached to the network that are distinguishable from desktops, laptops, or servers that have user accounts).

No

Comments:

We determined through interviews and our independent vulnerability scanning process that OPM does not maintain an accurate centralized inventory containing all servers and databases that reside within the network.

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

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

N/A

Section 4: Incident Response and Reporting

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

Yes

Section 4: Incident Response and Reporting

- 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).
No

Comments:

OPM owns a tool with the ability to automatically detect and report potential security incidents by analyzing data from various sources. After analyzing the data, the tool alerts security analysts to potential security incidents. However, the tool needs to be configured to collect relevant and meaningful data so the potential security alerts contain fewer false-positives. The OPM systems currently providing data to the security information and event management (SIEM) tool are over-reporting log and event data, which results in an excessive amount of data for security analysts to review. The number of alerts that security analysts must review and identify as false-positive creates a backlog that could cause a delay in identifying and responding to actual incidents.

- 4.1.6 Is capable of tracking and managing risks in a virtual/cloud environment, if applicable.
Yes
- 4.1.7 Is capable of correlating incidents.
Yes

Section 4: Incident Response and Reporting

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).

No

Comments:

OPM owns a SIEM tool with the technical ability to automatically detect, analyze, and correlate potential security incidents over time. However, the correlation features of this tool are not fully utilized at this time. This tool only receives event data from approximately 80 percent of major OPM information systems. In FY 2014, the OCIO established an Enterprise Network Security Operations Center (ENSOC) that provides continuous centralized support for OPM's security incident prevention/management program. However, the ENSOC cannot adequately fulfill its purpose if it does not receive data from all OPM systems.

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

N/A

Section 5: Risk Management

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

No

Comments:

In FY 2011, the OCIO organized a Risk Executive Function comprised of several IT security professionals. However, as of the end of FY 2014, 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. Also, of the 21 OPM systems due for Authorization in FY 2014, 11 were not completed on time and are currently operating without a valid Authorization. We believe that the volume and sensitivity of OPM systems that are operating without an active Authorization represents a material weakness in the internal control structure of the agency's IT security program.

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

Yes

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.
Yes
- 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.
Yes
- 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: Only 37 out of OPM's 47 systems were subject to adequate security controls testing in FY 2014.

- 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, SP 800-37).

No

Comments: The Authorization packages reviewed as part of this FY 2014 audit generally maintained the same satisfactory level of quality that had been observed in recent years. However, of the 21 OPM systems due for Authorization in FY 2014, 11 were not completed on time and are currently operating without a valid Authorization. The drastic increase in the number of systems operating without a valid Authorization is alarming, and represents a systemic issue of inadequate planning by OPM program offices to authorize the information systems that they own. We believe that the volume and sensitivity of OPM systems that are operating without an active Authorization represents a material weakness in the internal control structure of the agency's IT security program.

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

No

Comments: See comment in 5.1.15

Section 5: Risk Management

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

N/A

Section 6: Security Training

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

Yes

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.

N/A

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

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

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

Yes

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

Yes

7.1.2 Tracks, prioritizes, and remediates weaknesses.

Yes

7.1.3 Ensures remediation plans are effective for correcting weaknesses.

Yes

7.1.4 Establishes and adheres to milestone remediation dates.

No

Comments:

Our review indicated that many system owners are not meeting the self-imposed remediation deadlines listed on the POA&Ms. Out of OPM's 47 operational systems, 38 have POA&M items that are greater than 120 days overdue.

7.1.5 Ensures resources and ownership are provided for correcting weaknesses.

Yes

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

No

Comments:

All known security weaknesses were appropriately incorporated to the system-specific POA&Ms for only 29 of OPM's 47 systems. This includes 14 of the 25 systems operated by OPM, and 15 of the 22 systems operated by a contractor.

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

Yes

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.

N/A

Section 8: Remote Access Management

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

Yes

8.1.1 Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST 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 SP 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:

In previous years, we discovered that remote access sessions do not terminate or lock out after [REDACTED] inactivity as required by FISMA. OPM has acknowledged the issue and stated that the weakness cannot be remediated until the VPN vendor releases a software update.

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.

N/A

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

Yes

Section 9: Contingency Planning

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 several 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 2014. We believe that this indicates that OPM does not have a FISMA-compliant enterprise-wide business continuity / disaster recovery program.

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 39 of 47 systems in FY 2014.

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

No

Comments:

We received updated contingency plans for 41 out of 47 information systems on OPM's master system inventory.

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

Yes

Section 9: Contingency Planning

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. 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 full functional test was performed in FY 2014. 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, we received evidence that contingency plans were tested for only 39 of 47 systems in FY 2014.

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

No

Comments:

As mentioned in 9.1.5, we only received that 41 or 47 system have documented contingency plans.

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.

N/A

Section 10: Contractor Systems

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

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).(Base)

No

Comments:

We were provided evidence that the security controls were tested for only 19 out of OPM's 22 contractor operated systems.

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.

No

Comments:

The OCIO maintains a separate spreadsheet documenting interfaces between OPM and contractor-operated systems and the related Interconnection Security Agreements (ISA). However, many of the documented ISAs have expired.

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

Yes

Section 10: Contractor Systems

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.

No

Comments:

Of the 21 OPM systems due for Authorization in FY 2014, 11 were not completed on time and are currently operating without a valid Authorization. Three of the 11 are contractor-operated systems.

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

N/A

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

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.

N/A



Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: <http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse>

By Phone: Toll Free Number: (877) 499-7295
Washington Metro Area: (202) 606-2423

By Mail: Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100

-- CAUTION --

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