Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT

FY 2013

WASHINGTON, D.C.

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

Date: November 21, 2013

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

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

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

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

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

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

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

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