Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT

FY 2012

WASHINGTON, D.C.

Report No. 4A-CI-00-12-016

Date: 11/05/12

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

The Office of the Chief Information Officer (OCIO) has recently made noteworthy improvements to OPM's IT security program. The OCIO has increased staffing levels in its IT Security and Privacy Group, and has had a stable Chief Information Security Officer for the past two and a half years. The OCIO has also successfully addressed a significant number of long-standing IT audit recommendations. However, it is clear that there are still opportunities for improvement in the overall management of OPM's IT security program.

In FY 2007 and FY 2008, we reported a material weakness in controls over the development and maintenance of OPM's IT security policies. In FY 2009, we expanded the material weakness to include concerns with the agency's overall information security governance and its information security management structure. This material weakness was rolled forward through FY 2010. In FY 2011, the OCIO updated its IT security and privacy policies, but made little progress in

addressing our concerns with OPM's security management structure. Throughout FY 2012, the OCIO continued to operate with a decentralized IT security structure that did not have the authority or resources available to adequately implement the new policies.

In August 2012, the OPM Director issued a memo to Associate Directors and Office Heads notifying them that IT security responsibilities would be centralized under the OCIO effective October 1, 2012. The OCIO has begun hiring IT security professionals to manage the security of OPM's major information systems. Once this transition is fully complete, we expect to close the audit recommendations related to IT security governance and remove the material weakness. However, the material weakness remains open in this report, as the agency's IT security function remained decentralized throughout the FY 2012 FISMA reporting period and because of the continuing instances of non-compliance with FISMA requirements.

The OCIO's response to our draft audit report indicated that they disagree with the classification of the material weakness because of the progress that OPM has made with its IT security program and because there was no loss of sensitive data during the fiscal year. However, the OCIO's statement is inaccurate, as there were in fact numerous information security incidents in FY 2012 that led to the loss or unauthorized release of mission-critical or sensitive data. Several of these security incidents were reported by the media. In addition, these incidents led to financial loss to the agency in the form of credit monitoring services paid for individuals affected by OPM's loss of their sensitive data.

In FY 2010, we added a second material weakness related to the management of the Certification and Accreditation process (now referred to as Security Assessment and Authorization or Authorization). In FY 2011, the OCIO improved its Authorization policies and templates, and added additional resources to facilitate the Authorization process. These improvements warranted reducing the material weakness related to Authorizations to a significant deficiency in the FY 2011 FISMA report. In FY 2012, we observed continued improvement in the OCIO's management of the Authorization process, and no longer consider this issue to be a significant deficiency.

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

- 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. However, Oracle databases 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.