UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

FEDERAL INFORMATION SECURITY MANAGEMENT ACT AUDIT
FY 2010

WASHINGTON, D.C.

Report No. **4A-CI-00-10-019**

Date: 11/10/10

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 Inspector General (OIG) has significant ongoing concerns regarding the overall quality of the information security program at OPM.

In fiscal year (FY) 2007 and FY 2008 we reported a material weakness in controls over the development and maintenance of OPM's information technology (IT) security policies. In FY 2009, we issued a Flash Audit Alert to OPM's Director highlighting our concerns with the agency's IT security program. We also expanded the material weakness related to IT security policies to include concerns with the agency's overall information security governance and its information security management structure.

Although we acknowledge that some limited progress was made in FY 2010 to improve OPM's security program, we continue to consider the IT security management structure, insufficient

staff, and the lack of policies and procedures to be a material weakness in OPM's IT security program.

In addition, we are adding a second material weakness related to the management of OPM's Certification and Accreditation (C&A) process. The C&A concerns were reported as a significant deficiency in the FY 2008 and FY 2009 Federal Information Security Management Act (FISMA) audit reports. Specifically, we noted that not all systems at OPM have an active C&A, there is a wide range of quality in the C&A packages from various program offices, and the Office of the Chief Information Officer (OCIO) does not have the resources to facilitate the C&A process.

The agency has recently appointed a new Senior Agency Information Security Official. However, it remains to be seen whether it will commit the necessary resources and develop the appropriate functions required of this role. We will reevaluate this issue during the FY 2011 FISMA audit.

In addition to the material weaknesses describe above, the OIG noted the following controls in place and opportunities for improvement:

- The OIG does not agree with the number of systems identified in OPM's master system inventory. The OCIO takes a passive approach to maintaining the inventory, increasing the risk that applications containing sensitive data are operating in a production environment without being subject to the IT security controls required by FISMA.
- The OCIO does not maintain a single centralized inventory of the computer hardware in its data centers.
- The OCIO has developed a Windows XP image that is generally compliant with Federal Desktop Core Configuration standards. However, this image has not been implemented on any production workstations.
- The OCIO has developed thorough incident response and reporting capabilities.
- The OCIO has implemented a process to provide annual IT security and privacy awareness training to all OPM employees and contractors. However, controls related to providing specialized security training to individuals with information security responsibility could be improved.
- A Plan of Action and Milestones (POA&Ms) should be continuously managed for all agency systems, but we found that POA&Ms were updated every quarter in FY 2010 for only 35 of OPM's 43 systems.
- All 30 of the recommendations from the FY 2009 FISMA audit were appropriately incorporated into the OCIO POA&M. However, POA&M items from the system-specific audits conducted by the OIG do not appear in the POA&M of the individual systems.
- The POA&Ms for 9 OPM systems contain security weaknesses with remediation activities over 120 days overdue.
- [redacted]