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 2009

WASHINGTON, D.C.

Report No. 4A-CI-00-09-031

Date: November 5, 2009

This final audit report documents the Office of Personnel Management's (OPM's) continued efforts to manage and secure its information resources. We have significant concerns regarding the overall quality of the information security program at OPM. These concerns are rooted in the lack of adequate information security governance activities in accordance with legislative and regulatory requirements. Specifically, the agency has not fully documented information security policy and procedures or established appropriate roles and responsibilities.

The lack of policies and procedures was reported as a material weakness in the fiscal year (FY) 2007 and FY 2008 Federal Information Security Management Act (FISMA) audit reports. While some progress was made in FY 2009, detailed guidance is still lacking. An updated Information Security and Privacy Policy was finalized in August 2009. This policy outlines the information technology (IT) security controls that should be in place for the major applications owned by the agency. However, the majority of the text in this policy is derived or copied directly from National Institute of Standards and Technology (NIST) guidance and has not been tailored to specifically address OPM's IT environment. In addition, detailed procedures and implementing guidance are still missing.

This year we are expanding the material weakness to include the agency's overall information security governance program and incorporating our concerns about the agency's information security management structure. As of late September 2009, there had been no permanent senior agency information security official (SAISO) in the agency for nearly 18 months. During this time, we observed a serious decline in the quality of the agency's information security program. In addition, there is no permanent Privacy Program Manager assigned to manage the agency's privacy program. As a result, there are many deficiencies in OPM's privacy program.

The agency has recently appointed a new SAISO; 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 2010 FISMA audit.

The continuing weaknesses in OPM's information security program result directly from inadequate governance. Most, if not all, of the exceptions we noted this year resulted from a lack of necessary leadership, policy, and guidance. Our most notable observations include:

- As noted above, OPM continues to lack adequate and up-to-date IT security policies and procedures. We continue to consider this to be a material weakness in OPM's IT security program.
- One system on OPM's inventory was placed into production before a certification and accreditation (C&A) was completed, and the prior C&A for three systems has expired and a new C&A has not been completed. Weaknesses in OPM's C&A process continue to remain a significant deficiency in OPM's IT security program.
- Weaknesses in OPM's privacy impact assessment (PIA) process and the agency's failure to meet privacy-related requirements from the Office of Management and Budget (OMB) lead us to believe that there is a significant deficiency in OPM's management of its privacy program.

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

- OPM's Center for Information Services (CIS) maintains a master inventory of OPM's major systems. We generally agree with the number of systems listed in the inventory (42), but we identified at least one major application that does not appear on the system inventory and has not been subject to a C&A. In addition, OPM's system inventory does not identify interfaces between internal and external systems.
- A C&A has been completed and remains active for 38 of the 42 systems in OPM's inventory.
- The IT security controls have been adequately tested for 40 of OPM's 42 systems during FY 2009.
- Four out of OPM's 42 systems did not have an adequately documented and/or up-to-date contingency plan. In FY 2009, the contingency plans for 31 of OPM's 42 systems were tested in full compliance with the requirements of NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems.