Report In Brief

NOVEMBER 10, 2011

Why We Did This Review

Information security program, evaluation, and reporting requirements for federal agencies are established by The Federal Information Security Management Act of 2002 (FISMA). FISMA requires agencies to secure their information systems through the use of cost-effective management, operational, and technical controls. FISMA also requires inspectors general to evaluate agencies' information security programs and practices by assessing a representative subset of agency systems, and to report the results to the Office of Management and Budget (OMB) and Congress annually.

Background

The Department of Commerce's 280 information technology (IT) systems process, store, and transmit census, economic, trade, satellite, and weather data, among others, in support of its varied missions. This year, we assessed the security of 10 information systems selected from three Commerce operating units: five from the National Oceanic and Atmospheric Administration (NOAA), three from the U.S. Patent and Trademark Office (USPTO), and two from the Census Bureau.

In our FY 2010 FISMA audit, we concluded that the Department had not adequately secured its information systems. The Department concurred with our recommendations and developed an action plan to address them—but had not completed the actions by the FY 2011 audit.

OFFICE OF THE SECRETARY

FY 2011 Federal Information Security Management Audit: More Work Needed to Strengthen IT Security Department-Wide

OIG-12-007-A

WHAT WE FOUND

We identified deficiencies in fundamental aspects of security planning and significant security control weaknesses. These include continued failure to implement key controls that govern system access, securely configure components, patch vulnerable software, and audit and monitor system events. Flaws remain in the Department's process for reporting and tracking the remediation of IT security weaknesses. Overall, the entire Department needs to manage information security with greater rigor and consistency.

Specifically, we found deficiencies in:

- security planning that inhibit effective implementation of security controls;
- critical controls thus placing the department's systems at risk; and
- the Department's Plan of Action and Milestones (POA&M) process that undermine effective remediation of security weaknesses.

WHAT WE RECOMMENDED

To make the Department's information security program and practices more effective, the Department should:

- Complete actions planned in response to our FY 2010 FISMA audit, as quickly as possible.
- Develop a security planning checklist, or other planning tool, to help system owners and authorizing officials complete and maintain comprehensive security plans.
- Determine the feasibility of independent reviews at key steps in the risk management framework to ensure greater rigor and consistency in the security authorization process within the Department's various operating units. Consideration should be given to creating independent review teams with representatives from different operating units to share best practices and promote consistent application of Department policy.