Report In Brief

U.S. Department of Commerce, Office of Inspector General

November 15, 2010

Why We Did This Review

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to secure their information systems, commensurate with the risk of loss or unauthorized use of system data. Inspectors general must annually evaluate agency information security programs by assessing a representative sample of such systems, and reporting the results to the Office of Management and Budget (OMB) and to Congress.

Background

The Department and its operating units use over 300 information technology (IT) systems; this year we assessed security controls of 18 systems, from six different operating units.

Security weaknesses have been a long-standing problem for Commerce, particularly with respect to security planning, configuration settings, and control assessments. This year's review focused on Department-wide issues that require policy improvements and increased management attention.

Office of the Secretary

Federal Information Security Management Act Audit Identified Significant Issues Requiring Management Attention (OIG-11-012-A)

What We Found

The Department's information security program and practices are not adequately securing Department systems, and we are concerned that the likelihood and severity of security breaches are considerably greater than what is currently perceived by management. The following table summarizes our major audit findings:

Measure	Finding
High-risk vulnerabilities identified?	Extensive vulnerabilities in system software suggest considerable likelihood of a security breach; patch management and vulnerability scanning practices are not effective. Scans identified significantly more high-risk vulnerabilities than were previously known.
Configuration settings defined and documented?	Only 4 of 18 systems (one high-impact) adequately defined and documented secure settings for operating systems and major applications. This is a long-standing deficiency in a crucial security practice.
Configuration settings securely implemented?	Only one system securely configured settings for its operating systems.
Security weaknesses and corrective actions adequately reported and tracked?	Most systems exhibited significant deficiencies in reporting and tracking security weaknesses. As a result, the information about corrective action that the Department is using for performance measurement is inaccurate and inconsistent.
Contingency plans adequately tested?	Six of 18 systems' contingency plans were inadequately tested, including 2 systems that support the primary mission-essential weather forecasting function; testing of these 2 systems' contingency plans had not been done since FY 2007.
Alternate processing sites arranged?	Five systems that are required to have alternate processing sites do not have them, including three systems—two high-impact and one moderate-impact—that support weather forecasting. Documents attribute the lack of alternate sites primarily to budget constraints.

What We Recommend

We recommend that the Department revise its information security policy by providing specific implementation guidance that will ensure better and more consistent practices across the Department. Further, increased management attention is required to ensure that the deficiencies identified are rectified Department-wide.