Report In Brief

U.S. Department of Commerce, Office of Inspector General
August 2009

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

FY 2009 FISMA Assessment of Application Systems and Databases (OSE-19512)

Why We Did This Review

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to identify and provide security protection of information collected or maintained by it or on its behalf. Inspectors general are required to annually evaluate agencies' information security programs and practices. Such evaluations must include testing of a representative subset of systems and an assessment, based on that testing, of the entity's compliance with FISMA and applicable requirements.

This review covers our assessment of the certification and accreditation of the National Institute of Standards and Technology's (NIST) Application Systems and Databases system.

Background

Three elements are necessary for a system to be accredited: a system security plan, a security assessment report, and a plan of action and milestones. Further, the Department's information technology (IT) security standards require documented evidence of the assessment's adequacy in the form of the certification test plan and the certification test results.

What We Found

While some deficiencies were noted with security planning prior to the certification phase, NIST's certification and accreditation process—in particular, its assessment of security controls—did produce sufficient information for the authorizing official to make a credible, risk-based decision to approve system operation.

At the same time, however, NIST's security planning process needs improvement, secure configuration settings had not been established for all information technology (IT) products, some minor improvements are necessary in control assessments, and we found specific vulnerabilities requiring remediation.

What We Recommend

We are making several recommendations, including those dealing with security planning steps, correction of identified deficiencies, conformance with NIST guidance, post-remediation testing, and continuous monitoring. NIST concurred with most of our findings and recommendations, but disagreed that its security plan had actually been written by the certification team. Further, its remarks on two deficiencies that we noted were nonresponsive to our concerns.