Report In Brief

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

August 2009

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) Manufacturing Engineering Laboratory Managed Infrastructure.

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.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

FY 2009 FISMA Assessment of the Manufacturing Engineering Laboratory Managed Infrastructure (OSE-19511)

What We Found

In general, our review was quite positive. Due in part to the departmental Chief Information Officer's *Smart Spot Check* and subsequent improvement to the certification and accreditation, the authorizing official did receive sufficient information to make a credible, risk-based decision to approve system operation. Moreover, continuous monitoring is providing important data about the operational status and effectiveness of security controls.

We noted only minor deficiencies, including (1) needed improvements in the system security plan; (2) the need for secure configuration settings for applications; (3) some certification weaknesses in control assessments; and (4) vulnerabilities uncovered by our assessments that require remediation.

What We Recommend

Our recommendations concern documentation, conformance with NIST guidance, the application of security controls to all relevant information technology (IT) products, reflecting identified vulnerabilities in its plan of action and milestones, and correction of noncompliant system configuration settings. NIST fully concurred with our findings and with all but one recommendation.