Report In Brief

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

September 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 Bureau of Industry and Security's (BIS) continuous monitoring of its information technology (IT) infrastructure system since its accreditation in 2006.

Background

Continuous monitoring is a critical post-accreditation aspect of the security certification and accreditation process. Effective continuous monitoring requires configuration management and control of information system components, security impact analyses of changes to the system, assessment of security controls, and status reporting.

We sought to determine whether, due to continuous monitoring, (1) officials are kept informed about the status and effectiveness of security controls, (2) the agency promptly mitigates any deficiencies, and (3) BIS has resolved deficiencies we noted in our FY 2006 evaluation.

BUREAU OF INDUSTRY AND SECURITY

FY 2009 FISMA Assessment of BIS Information Technology (IT) Infrastructure (OSE-19574)

What We Found

Continuous monitoring has not been conducted since the 2006 accreditation. Further, significant certification and accreditation deficiencies that we previously identified have not been corrected. Our on-site review this year found other vulnerabilities that likewise require remediation. As a result, officials have no assurance that the required controls are in place to adequately protect the IT infrastructure system and its information. Although the authorization to operate the system expired earlier this year, BIS has no current plans to reaccredit its IT system. Thus, BIS should not have reported to the Office of Management and Budget and the Department that annual assessments of security controls were conducted or that the system was certified and accredited.

BIS officials provided no explanation as to why these actions have not been taken. Until such protections are in place, this system will remain vulnerable.

What We Recommend

We are making many specific recommendations aimed at putting into place a system in which changes are documented, monitoring of selected security controls is continuous, and authorizing officials are informed of and accept necessary risks. BIS officials have indicated their agreement with our findings and recommendations.