Report In Brief

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

September 2009

BUREAU OF INDUSTRY AND SECURITY

FY 2009 FISMA Assessment of Bureau Export Control Cyber Infrastructure, Version 2 (OSE-19575)

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 Bureau of Industry and Security's (BIS) Export Control Cyber Infrastructure (ver. 2).

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

The certification and accreditation of the Bureau Export Control Cyber Infrastructure (ver. 2) did not meet Department or FISMA requirements. Security planning deficiencies--in particular, the lack of defined security requirements--undermined the certification team's ability to assess controls accurately and completely.

We found that (1) key security planning activities necessary for certification and accreditation were not performed, (2) secure configuration settings were not defined for IT products prior to the security control assessment, (3) the security control assessment was not adequate, (4) the authorizing official's accreditation decision violated Department and BIS IT security policy and FISMA guidance, (5) reporting procedures required by Department IT policies were not followed, and (6) our control assessment found vulnerabilities requiring remediation.

What We Recommend

We are making many specific recommendations aimed at improving the bureau's certification and accreditation process, and bringing it into conformance with both FISMA and departmental requirements. We are also recommending that BIS address the vulnerabilities that we found in our on-site assessment of security controls. According to its Acting Chief Information Officer, the bureau agrees with our findings and recommendations.