Report In Brief

OCTOBER 16, 2015

BUREAU OF INDUSTRY AND SECURITY

Lack of Basic Security Practices Hindered BIS' Continuous Monitoring Program and Placed Critical Systems at Risk

OIG-16-003-A

Background

A continuous monitoring program and strategy, required in accordance with Office of Management and Budget (OMB) and Departmental requirements, allows an organization to maintain ongoing awareness of information security vulnerabilities and threats to support organizational risk management decisions. Key components of continuous monitoring are (1) keeping management aware of the current security state of information systems, and (2) supporting the processes of ongoing authorization and near-real-time risk management.

Why We Did This Review

We conducted this audit to determine whether BIS' continuous monitoring strategy and practices, including ongoing security control assessments of its critical information systems, provide adequate information for authorizing officials to make proper risk-based decisions.

We evaluated BIS' continuous monitoring program, including strategy and implementation. We also performed our own assessments of selected critical security controls in place to protect two of BIS' high-impact systems designed to support its mission to advance U.S. national security, foreign policy, and economic objectives: the BIS Export Control Cyber Infrastructure Version 2 and the Investigative Management System Redesign. We also reviewed BIS' compliance with a number of applicable provisions of law, regulation, and mandatory guidance of, among others, the Federal Information Security Management Act of 2002 (FISMA), IT Security Program Policy, NIST Federal Information Processing Standards, and Special Publications.

WHAT WE FOUND

BIS' documented strategy for continuous monitoring was in compliance with Department policy and NIST guidance. However, we found that

Deficient vulnerability scanning practices increased compromise risk. Effective vulnerability scanning supports an organization's continuous monitoring program by allowing the organization to identify vulnerabilities on an ongoing basis. We evaluated BIS' vulnerability scanning practices for its high-impact systems and found significant deficiencies. Specifically, we found that (a) an outdated vulnerability scanning tool was used to identify security weaknesses, (b) required credentialed vulnerability scans were not always performed, (c) vulnerability scanning results were not reviewed to determine remediation actions, and (d) BIS had no assurance that all system components were scanned for vulnerabilities.

BIS had no assurance that security weaknesses were remediated. Federal agencies are required to use plans of action and milestones (POA&Ms) to track corrective actions to remediate security weaknesses. In order to create transparency, accountability, and oversight, the Department requires that bureaus use the Department's Cyber Security Assessment and Management (CSAM) tool and follow a standard POA&M process. However, we found that BIS neither consistently followed the required process nor used the required tool to ensure that security weaknesses were remediated. In fact, not only did BIS not take corrective action to address basic IT security weaknesses for over 5 years, it also did not always develop POA&Ms in CSAM to track the known security weaknesses, resulting in avoidance of Department oversight. Furthermore, BIS did not clearly define responsibilities for remediating vulnerabilities.

WHAT WE RECOMMEND

We recommend that the Under Secretary for Industry and Security direct BIS' acting chief information officer to

1. ensure that an accurate inventory of hardware components and software products that make up its systems is established and maintained.
2. establish an effective vulnerability scanning procedure that requires scanning all components in BIS's inventory, updating the vulnerability scanning tool regularly, using credentials for scanning, and reviewing vulnerability scanning reports in a timely manner.
3. ensure that responsibility for vulnerability remediation, including patching, for BIS system components, is clearly documented.
4. ensure that POA&Ms are created for all un-remediated security weaknesses.
5. implement procedures to provide accountability and greater management oversight of the POA&M process, and ensure supporting artifacts to be included in the POA&Ms.