Report In Brief

SEPTEMBER 27, 2012

Background

The International Trade Administration (ITA) helps improve the global business environment—and U.S. companies compete at home and abroad—through export promotion and commercial diplomacy, as well as shaping trade policy, market access, and enforcement of U.S. trade laws.

To fulfill its critical missions ITA heavily relies on information technology (IT), particularly the Internet, to conduct its business, and inevitably faces greater cybersecurity risks. In recent years, ITA has become a frequent target of cyber attacks. In order to minimize the serious damage caused by cyber attacks, ITA has taken action such as consolidating Internet access through a centralized service.

Why We Did This Review

The Federal Information Security Management Act of 2002 (FISMA) requires agencies to secure systems against the loss, misuse, or unauthorized access to or modification of information collected or maintained by, or on behalf of, an agency. In addition, FISMA requires inspectors general to evaluate agencies' information security programs and practices by assessing a representative subset of agency systems, with results reported to the Office of Management and Budget (OMB), Department of Homeland Security, and Congress annually.

As part of an overall assessment of the Department's IT security program, we evaluated information security controls and security-related documentation for six ITA systems. Our objective was to determine whether key security measures adequately protect ITA's systems and information.

INTERNATIONAL TRADE ADMINISTRATION

Improvements Are Needed to Strengthen ITA's Information Technology Security Program

OIG-12-037-A

WHAT WE FOUND

We found weaknesses in the six ITA systems we reviewed, including *inadequate security categorization* that may affect protection against critical information and security control deficiencies that increase the likelihood of a successful cyber attack. The security control deficiencies include (a) *deficiencies with vulnerability scanning and patch management*, (b) *weaknesses in securing databases*, (c) *the presence of unauthorized software and use of unauthorized removable media*, and (d) *risks related to network implementation*:

Deficiencies with vulnerability scanning and patch management. ITA's vulnerability scanning of system components and patch management for software products do not effectively identify or remediate security weaknesses.

Weaknesses in securing databases. ITA improperly configured one database to use a blank password for authentication to a database administrator account. We also identified three additional improperly configured databases that, if exploited, could allow excessive privileges to access sensitive information.

The presence of unauthorized software and use of unauthorized removable media. ITA has unauthorized software on its network and lacks controls to prevent the use of unauthorized USB devices, thus opening its systems to additional risks, such as information exfiltration.

Risks related to network implementation. ITA's network implementation allows network traffic to flow freely between computing components, which could pose a greater security risk on ITA systems and information.

WHAT WE RECOMMEND

We recommend that the Under Secretary of Commerce for International Trade:

1. Ensure that system owners and appropriate ITA officials collaborate to identify and categorize all information processed, stored, or transmitted by each system and categorize each system accordingly;
2. Mitigate the remaining vulnerabilities identified by our vulnerability scan assessments;
3. Improve the patch management process by (a) making timely patches for all software products and (b) coordinating within ITA to comprehensively identify and remediate software flaws in a timely manner;
4. Address and fully implement critical security settings in database configuration checklists;
5. Ensure that only authorized software and USB devices are used on both servers and workstations; and
6. Strengthen the worldwide enterprise network's security posture by reducing the threats associated with allowing network traffic to flow freely between all computing components.