Report in Brief

March 27, 2018

Background

The International Trade Administration (ITA) strengthens the competitiveness of U.S. industry, promotes trade and investment, and ensures fair trade through the rigorous enforcement of our trade laws and agreements.

To support the mission, ITA heavily relies on cloud computing services for its information systems. The Department and its bureaus are required to follow federal laws to secure information technology (IT) systems through the use of cost-effective management, operational, and technical controls.

This responsibility applies to all IT systems, including those using cloud computing services. Furthermore, since 2010, federal agencies have been directed to follow the National Institute of Standards and Technology's (NIST's) six-step process in managing risks throughout an information system's life cycle, known as the Risk Management Framework (RMF). This framework includes security categorization, control implementation and assessment, and system authorization according to a risk-based decision.

Why We Did This Review

We conducted this audit to determine whether key security measures are in place to adequately protect ITA systems that utilize cloud computing services.

INTERNATIONAL TRADE ADMINISTRATION

ITA Needs a Stronger Commitment to Safeguard Its Cloud-Based Systems

OIG-18-017-A

WHAT WE FOUND

We found that ITA was unaware of significant weaknesses in the process of authorizing systems into operations, as well as maintaining and safeguarding its cloud-based systems. Specifically,

1. *ITA used a deficient process for system security categorization.* We found that the authorizing official had no involvement in the security categorization process, and ITA inadequately implemented a process for identifying and categorizing information on its systems.
2. *ITA did not adequately secure its cloud infrastructure.* We found that cloud infrastructure user access controls were not in compliance with the Department requirements, unrestricted network access to virtual servers was allowed, and excessive file permissions were configured on cloud storage.
3. *ITA failed to implement fundamental security controls on its systems.* We found that vulnerability scanning practices were inadequate to identify vulnerabilities, critical vulnerabilities were not remediated in a timely manner, ITA was unaware of network services on undocumented open ports, and information systems did not have system-level contingency plans.

WHAT WE RECOMMEND

We recommend that the Under Secretary for International Trade direct the ITA Chief Information Officer to

1. Follow the NIST RMF to revalidate all the security categorizations for ITA systems, including identifying all information types and providing sufficient justification if deviating from the NIST provisional categorization level; ensure system owners, information owners, information system security officers, and system technical leads are sufficiently familiar with the NIST RMF to conduct the security categorization process.
2. Establish a reporting mechanism to ensure that ITA's authorizing official correctly reviews and approves ITA's security categorization process. This mechanism should require control implementation assessors properly evaluate and report to ITA senior security officials whether ITA's security categorization process complies with NIST 800-53 requirements.
3. Ensure security controls are appropriately assessed and supported by sufficient evidence.
4. Periodically review the configuration of ITA cloud-based infrastructure to ensure that the configuration adheres to Department policies and encourage implementing industry best practices.
5. Establish a process to ensure effective coordination between the security and operation teams, and include maintaining a shared, accurate record of created and decommissioned virtual servers.
6. Use existing vulnerability scanning tools to include periodic database scans, and evaluate the use of additional web application scanning tools available through the Department Continuous Diagnostic and Mitigation (CDM) program.
7. Enhance ITA patching process by: (a) reconciling differences between management direction and ITA policy; (b) adhering to the Department patching timeframes; and (c) testing patches prior to deployment as required by Department policy.
8. Document and maintain a list of authorized ports for each ITA system and disable all unauthorized ports.
9. Establish contingency plans for each ITA system according to Department policy.