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

FINAL REPORT NO. OIG-18-017-A
MARCH 27, 2018

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

March 27, 2018

MEMORANDUM FOR: Gilbert Kaplan
Under Secretary for International Trade
International Trade Administration

FROM: Frederick J. Meny, Jr.
Director for Satellites and Weather Systems

SUBJECT: *ITA Needs a Stronger Commitment to Safeguard Its Cloud-Based Systems*
Final Report No. OIG-18-017-A

Attached is our final audit report conducted to determine whether key security measures are in place to adequately protect International Trade Administration (ITA) systems that utilize cloud computing services.

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, ITA (1) used a deficient process for system security categorization; (2) did not adequately secure its cloud infrastructure; and (3) failed to implement fundamental security controls on its systems.

On March 13, 2018, OIG received ITA's response that concurred with all of our draft report's findings and recommendations. We have summarized ITA's response and included its entire formal response as appendix C.

In accordance with Department Administrative Order 213-5, please submit to us an action plan that addresses the recommendations in this report within 60 calendar days. The final report will be posted on OIG's website pursuant to sections 4 and 8M of the Inspector General Act of 1978, as amended (5 U.S.C. App., §§ 4 & 8M).

We appreciate the cooperation and courtesies extended to us by your staff during our audit. If you have any questions or concerns about this report, please contact me at (202) 482-1931, or Dr. Ping Sun, Director for IT Security, at (202) 482-6121.

cc: Rod Turk, Acting Chief Information Officer
Rand Ruggieri, Acting Chief Information Officer, ITA
Jennifer Eveland, Audit Liaison, ITA
Joe Ramsey, Audit Liaison, ITA
Maria Dumas, Audit Liaison, Office of the Chief Information Officer

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.

Contents

Cover: Herbert C. Hoover Building main entrance at 14th Street Northwest in Washington, DC. Completed in 1932, the building is named after the former Secretary of Commerce and 31st President of the United States.

Introduction

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. ITA works to improve the global business environment and helps U.S. organizations compete at home and abroad. To support this mission, ITA heavily relies on cloud computing services[1] for its information systems.

The Department and its bureaus are required to follow federal laws to secure information technology (IT) systems[2] 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).[3] This framework includes security categorization, control implementation and assessment, and system authorization according to a risk-based decision.

[1] Cloud computing is a way for acquiring and delivering computing services. It enables on-demand access to shared computing resources with the goal of reducing information technology (IT) costs.
[2] Federal Information Security Modernization Act of 2014, Pub. L. No. 113–283, an update of the Federal Information Security Management Act of 2002, Pub. L. No. 107–347.
[3] NIST, February 2010. *Guide for Applying the Risk Management Framework to Federal Information Systems*, NIST SP 800-37, Rev 1. Gaithersburg, MD: NIST.

Objective, Findings, and Recommendations

We conducted this audit to determine whether key security measures are in place to adequately protect ITA systems that utilize cloud computing services. See appendix A for further details regarding our objective, scope, and methodology. We judgmentally selected 10 out of 19 systems that support ITA's critical mission (see appendix B). Two systems provide infrastructure support such as virtual servers, networking, and storage. The other 8 systems are applications that support ITA's mission. Our review focused on fundamental security practices and control implementations on these selected systems.

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, ITA: (1) used a deficient process for system security categorization; (2) did not adequately secure its cloud infrastructure; and (3) failed to implement fundamental security controls on its systems.

I. ITA Used a Deficient Process for System Security Categorization

In order to protect its systems, an organization first needs to consider all information that a system processes, stores, or transmits to determine risks to the system and then select appropriate security controls. This process is referred to as security categorization and is required by Federal Information Processing Standard (FIPS) 199. Security categorization identifies the impact level of a system as high, moderate, or low based on the potential impact to an organization, should an event jeopardize its information or information system. A system with a higher impact level requires the organization to implement more stringent security controls, compared to one with a lower impact level.

In 2012, we reviewed ITA's security categorization process and reported deficiencies.[4] In response to our recommendations, ITA made corrections to its categorization process. However, during our current audit we found new deficiencies in ITA's security categorization process. Specifically, 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. These deficiencies could result in disproportionate protection of information systems and place the systems and ITA's important assets at risk.

A. Authorizing Official Had No Involvement in the Security Categorization Process

NIST's security categorization process[5] provides a structured way to determine the criticality and sensitivity of the information being processed, stored, and transmitted by an information system. It is the first, fundamental step in the RMF and is crucial for proper system authorization by an authorizing official. Specifically, correctly selecting

[4] U.S. Department of Commerce, Office of Inspector General, September 27, 2012. *Improvements Are Needed to Strengthen ITA's Information Technology Security Program*, OIG-12-037A. Washington, DC: OIG.
[5] NIST, February 2004. *Standards for Security Categorization of Federal Information and Information Systems*, FIPS 199. Gaithersburg MD: NIST.

security controls to be implemented on a system directly correlates to the security impact level of the system, which is determined by the security categorization. Thus, the security categorization document is a fundamental part of a system authorization package.

According to the RMF, the authorizing official should carefully review and approve the security categorization document to ensure that the system authorization decision is made in accordance with the accurate system's security impact level. Therefore, the authorizing official involvement in the security categorization process is essential and required by federal standard.

However, ITA's authorizing official ignored this review and approval process. We reviewed ITA's most recent security authorization packages for 9 selected systems[6] and found that the authorizing official did not review or approve the categorization documents. In fact, we identified numerous gross errors in these categorization documents. For example, significant portions of the documents were left blank, and erroneous data was duplicated across multiple systems' documentation. When we asked the reason for lack of involvement in this process, ITA security staff acknowledged that they did not make it a priority to review and approve security categorization documents.

In addition, as required by the RMF, control implementation assessors must evaluate whether the security categorization process complies with the NIST standard and if the authorizing official has reviewed and approved the categorization decision. However, ITA's assessors did not identify this deficiency but reported that the process was sufficiently implemented.

B. ITA Inadequately Implemented a Process for Identification and Categorization of Information on Its Systems

To properly categorize an information system's security impact level, the organization must identify and categorize what type of information is processed, stored, or transmitted by the system. To facilitate this effort, NIST guidance provides a list of information types (e.g., contingency planning information type, enterprise architecture information type, global trade information type) and their corresponding provisional levels of high, moderate or low, for confidentiality, integrity, and availability.[7]

In responding to our recommendations made in 2012, ITA improved its categorization process by including the system owner, information owner, and information system security officer (ISSO) as part of the review. During this audit, these officials asserted that they used a list of NIST's information types and identified those that were processed, stored, and transmitted by each system. However, there was a clear

[6] The ITA Amazon Web Services Platform was not applicable to our FIPS 199 analysis.
[7] NIST, August 2008. *Guide for Mapping Types of Information and Information Systems to Security Categories*, 800-60, Vols. 1-2 Rev 1. Gaithersburg MD: NIST.

indication of confusion and hesitation to identify specific information types on ITA systems among these officials during our discussions with them.

For example, we asked the system owner whether the global trade information type[8] existed on an ITA mission critical system. Initially, the system owner responded that this information type existed on the system. But after we provided the NIST description of the global trade information type, the system owner and control implementation assessor stated that such information did not exist on the system. In later discussions, ITA's Chief Information Security Officer reverted back to their previous response and acknowledged that the global trade information type indeed existed on the system.

This example clearly demonstrates a lack of understanding of information types by ITA officials with responsibility for managing and operating ITA information systems. This lack of understanding is due in part to these officials not being aware of key NIST guidance for conducting the security categorization process.[9] Miscategorization, caused by this lack of understanding, could lead to inadequate security protection of ITA systems, resulting in unauthorized disclosure of sensitive business data and adversely affecting ITA's public trust.

We also found additional inadequacy in ITA's security categorization process. After identifying all information types for a system, ITA should assign provisional categorization levels for each information type based upon FIPS 199 and NIST guidance. For some information types, ITA downgraded its security impact level from NIST provisional levels[10], resulting in downgrading the entire system to a lower security impact level that required less security controls to be implemented. The management decision of deviating from the NIST provisional categorization requires documented justification. We reviewed ITA's justification and found it was insufficient to provide reasonable explanation. Specifically, the rationale for downgrading from a high impact level of a sensitive information type to moderate was made simply by stating that it met the minimum security requirement. Additionally, the rationale did not account for all sensitive information types on the system. For example, sensitive business proprietary information collected by one ITA system was not considered in ITA's categorization rationale. However, according to ITA operation officials, unauthorized release of this data can lead to commercial harm to U.S. businesses.

The inadequate security categorization of IT systems and its information could result in either over protection of information systems, which wastes valuable resources; or under protection, which places the information system and its important assets at risk. The insufficient involvement by ITA security staff and authorizing official compounds this risk.

[8] The global trade information type is defined by NIST 800-60, volume II as those activities the Federal Government undertakes to advance worldwide economic prosperity by increasing trade through the opening of overseas markets and freeing the flow of goods, services, and capital.
[9] See the footnote 4.
[10] Provisional impact levels (low, moderate, high, or not applicable values) are the suggested impact levels assigned to the confidentiality, integrity, and availability security objectives of an information type based upon NIST 800-60, volume II.

II. ITA Did Not Adequately Secure Its Cloud Infrastructure

Among the 10 ITA cloud-based systems we reviewed, 9 were using the Amazon Web Services (AWS) infrastructure as a service (IaaS). AWS provides necessary infrastructure services to its customers such as virtual servers, cloud storage and networking, and allows these services to be customized to meet the customers' needs for their systems hosted on AWS. Although AWS must meet the standard security requirements,[11] ultimately it is the customers' responsibility to securely configure their customized AWS cloud infrastructure services. Accordingly, ITA must assume this responsibility as required by Department policy.

In supporting the infrastructure services customization, AWS provides a web-based graphical interface for its customers to provision and configure these services. Additionally, to help AWS customers properly configure their infrastructure services, a best practice security benchmark has been established by the Center for Internet Security (CIS),[12] which is available through the AWS website. AWS customers can use this benchmark to check if their current AWS infrastructure configuration is adequately secured.

We assessed ITA's AWS infrastructure configuration against the Department policies and the CIS benchmark, and found that cloud infrastructure user access controls were not in compliance with the Department requirement. In addition, ITA allowed unrestricted network access to virtual servers and had excessive file permissions on cloud storage.

A. Cloud Infrastructure User Access Controls Were Not in Compliance with Department Requirements

In order to access the AWS web-based interface to configure its AWS cloud infrastructure services, ITA users have to authenticate via a user ID and password. The Department policy[13] establishes specific requirements for passwords, including prohibiting password reuse and changing the password every 90 days. We found that ITA password configuration of the AWS web-based interface did not meet these requirements. In addition, we reviewed ITA AWS infrastructure user accounts, and found 10 out of 45 user accounts were not active for over 90 days. The Department policy requires inactive user accounts to be disabled or removed after 30 days of inactivity.[14]

Preventing the reuse of a password, changing the password periodically, and disabling inactive accounts are among the best and yet fundamental security practices. By not following these best practices, ITA's AWS infrastructure is less resilient against

[11] A cloud service provider is required to be Federal Risk and Authorization Management Program (FedRAMP) compliant. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
[12] Center for Internet Security (CIS) develops best practice solutions for cyber defense. CIS benchmarks are the global standard and recognized best practices for securing IT systems and data against cyberattacks.
[13] DOC, September 2012. Commerce Information Technology Requirement (CITR)-021, Washington, DC: DOC.
[14] DOC, September 2014. *Department of Commerce Information Technology Security Program Policy* (ITSPP), Control AC-2.3, Washington, DC: DOC.

password attack, such as brute force[15] login attempts or using stolen passwords, and therefore increases risk of compromise, which could lead to a detrimental impact on ITA operations.

B. *Unrestricted Network Access to Virtual Servers Was Allowed*

ITA uses AWS cloud network services to host virtual servers for its systems on AWS cloud infrastructure. AWS cloud network services allow ITA to restrict network connections to the virtual servers, similar to a network firewall, to prevent its infrastructure from remote cyberattacks.

We reviewed the cloud network services configuration and found ITA granted unrestricted network connection for a remote console service running on two ITA virtual servers. This configuration allowed making unrestricted remote connection to console service on these virtual servers from any network. Further, if the remote console service was compromised, it could allow an attacker to execute commands on these virtual servers remotely, resulting in exfiltration of sensitive data or disruption of the cloud infrastructure operation.

The Department policy requires implementing the least functionality control, which is defined by NIST to provide only essential capabilities and restricts the use of the network services.[16] Unrestrictive remote connection to the virtual servers undermined an essential protection for ITA AWS infrastructure and could provide an easy conduit for attackers to launch cyberattacks.

C. *Excessive File Permissions Were Configured on Cloud Storage*

ITA stores backup data in the cloud using Amazon Simple Storage Service (S3). This service allows ITA to store files across 32 S3 buckets.[17] Each bucket can be configured to allow specific access permissions to the files stored within, such as read, write, or delete. ITA is responsible for ensuring that files in S3 buckets are only available to authorized users who have a need to access the files to accomplish specific tasks, as required by the Department policy and defined by NIST control requirement.[18] We assessed the access permissions of ITA's S3 buckets and found that five S3 buckets were configured to allow anyone to upload or delete data.

According to ITA officials, ITA relies on AWS to back up its data for all the systems hosted there. Excessive file permissions to the ITA S3 buckets could, accidentally by

[15] A brute-force attack is a type of malicious attack against a system in which the attacker repeatedly attempts to gain access by presenting all possible combinations of access credentials until a match is found. An attacker attempting to gain access to a system by guessing all possible combinations of characters in a password is an example of a brute-force attack.
[16] NIST, April 2013. *Security and Privacy Controls for Federal Information Systems and Organizations,* NIST 800-53, rev 4, security controls CM-7. Gaithersburg MD: NIST.
[17] A bucket is a logical unit of storage in AWS.
[18] NIST, April 2013. *Security and Privacy Controls for Federal Information Systems and Organizations,* NIST 800-53, rev 4, security controls AC-6. Gaithersburg MD: NIST.

users or intentionally by attackers, compromise integrity and availability of ITA backup data. This could result in ITA being unable to restore its operations in case of data loss.

Adequately securing a cloud infrastructure is a shared responsibility between ITA and the cloud service provider. While the cloud service provider must meet standard security requirements, as a customer, ITA bears indispensable responsibility to protect its cloud infrastructure, which provides underlying support for ITA systems. ITA management acknowledged these issues, and took action to remediate the identified deficiencies.

III. ITA Failed to Implement Fundamental Security Controls on Its Systems

We reviewed fundamental security controls on 10 selected cloud-based systems supported by 198 virtual servers. Eight of these systems are application systems and 2 are infrastructure systems. We found that ITA's vulnerability scanning practices were inadequate, and critical vulnerabilities were not remediated in a timely manner. In addition, we found unauthorized open ports on ITA systems that could increase the security risk of systems. Furthermore, ITA systems did not have required system-level contingency plans.

A. Vulnerability Scanning Practices Were Inadequate to Identify Vulnerabilities

Department policy requires that bureaus scan all network addressable devices, such as servers and workstations, at least quarterly.[19] We reviewed vulnerability scanning reports for the 10 selected systems covering the most recent two quarters and found that ITA did not scan 29 out of 198 virtual servers. Nineteen of these 29 virtual servers were not scanned because they were not added to the scanning target list when they were provisioned. This happened due to the lack of coordination between ITA's security group, which is responsible for scanning, and ITA's operations group, which is responsible for maintaining virtual servers. Five of the 29 virtual servers were being prepared for removal, and the remaining 5 could not be located by ITA staff. It was only after we provided additional details that ITA was able to identify the servers and found that they had been removed.

Additionally, we found that ITA did not perform database scans and its web application scans were not comprehensive. As part of this audit, we scanned databases using a specialized tool and identified critical and high-risk vulnerabilities unknown to ITA. We also conducted a web application vulnerability scan and identified a high-risk vulnerability that was not discovered by ITA's own web application scanning tools. ITA took immediate action to remediate the identified high-risk web application vulnerability after being notified.

B. Critical Vulnerabilities Were Not Remediated in a Timely Manner

Department policy requires that bureaus remediate vulnerabilities identified from vulnerability scanning in a timely manner, depending on the risk impact of the systems,

[19] DOC, January 25, 2012. Commerce Information Technology Requirement, Vulnerability Scanning and Patch Management, CITR-016. Washington, DC: DOC.

as defined by FIPS 199. Specifically, vulnerabilities shall be remediated within 60 days for moderate impact systems and 90 days for low impact systems.[20] We reviewed scanning reports for the 10 selected ITA moderate and low impact systems and found that ITA did not remediate in a timely manner. We identified 102 virtual servers that have a total of 513 critical and high-risk vulnerabilities[21] that were not remediated for over 150 days, which violates the Department policy.

Vulnerabilities could not be patched and remediated in a timely manner because, according to ITA officials, ITA did not have a technical capability to test patches prior to deploying them on the virtual servers.[22] However, when we briefed ITA about this issue, the ITA Chief Information Officer indicated that it was not necessary to test patches for critical vulnerabilities, and the patches should be immediately installed according to the ITA patching policy. However, we reviewed the policy[23] and found the requirement for immediate patching was not present, and instead, the policy did require testing of the patches. Clearly, there was a gap between what ITA management wants to do and what the ITA policy requires with vulnerability patching process, which may be another contributing factor for deficient vulnerability remediation. By not patching vulnerabilities on the servers in a timely manner, ITA left its system vulnerable to potential cyberattacks.

C. ITA Was Unaware of Network Services on Undocumented Open Ports

In general, a network service is an application on a computer that accepts communication from another computer on the network. Each individual network service uses a designated network port number. For example, a web service usually uses port number 80. When a network service is waiting to accept connections, also known as "listening" on a port, this port is considered open on the computer. The open ports that are needed to support system functions (e.g., web, email, and remote file transfer services) should be authorized and maintained in the system's security documentation.

ITA did not document and authorize any open ports and services currently being used on its systems. Federal agencies are required to adhere to the security control requirements defined by NIST, which include documenting ports and services that are necessary for operations. This documentation can help system personnel disable all unneeded ports and services, thus limiting information systems to the least functionality necessary. Because open ports and running services were not documented, ITA is unable to properly limit functionality, which increases the risk of potential cyberattack.

By reviewing the ITA scanning reports, we found that a large number of open ports existed on servers hosted on ITA's AWS IaaS. We provided our analysis results of these

[20] DOC, January 25, 2012. Commerce Information Technology Requirement, Vulnerability Scanning and Patch Management, CITR-016. Washington, DC: DOC.
[21] For example, if exploited, a critical or high vulnerability could allow an attacker to execute arbitrary commands or gain unauthorized access to protected data on the affected server.
[22] Testing patches before deployment aids in preventing issues with software conflicts in the production environment which could cause a disruption in an organization's business operation.
[23] ITA's vulnerability management policy meets Departmental requirements.

open ports to ITA and asked them to validate whether these ports were needed on the systems. ITA confirmed that there were at least 60 unique open ports. Among them, 54 were being used for the ITA operation, but the remaining 6 ports were unaccounted for. Among these 6 unaccounted open ports, 2 existed on multiple servers: 1 on 26 servers and 1 on 149 servers. The remaining 4 ports were found on a single server. ITA was not able to determine what network services were listening on those ports. Unknown services listening on open ports are a characteristic of potential malicious activity and could provide attack avenues into ITA systems.

D. Information Systems Did Not Have System-level Contingency Plans

Department policy states that information systems need an established contingency plan. Such a plan should address maintaining essential missions and business functions despite an information system disruption, compromise, or failure. The plan should also address full information system restoration without deterioration of its security.[24]

We found that ITA did not establish contingency plans for 9 of the 10 systems we selected for review. The remaining one was outside of ITA's scope of responsibility due to the nature of the Software as a Service (SaaS)[25] cloud model. When we requested documentation related to contingency planning, we received documented procedures for only 5 of 9 applicable systems. Of the 5 system documents provided, 2 were outdated and no longer applicable to recovering the system.

When we inquired how ITA would address such outages, ITA management asserted that the systems hosted on the IaaS cloud were legacy systems and not crucial to ITA operations. Therefore, restoration of these systems was not a priority. However, we found that ITA currently relies on 1 system to conduct important anti-dumping investigations. Furthermore, another ITA system hosts Active Directory[26] servers, which authenticate and grant access to the ITA network and systems. Without the Active Directory servers, no one at ITA can conduct their daily business operations, such as accessing network resources and email communication. ITA needs to ensure that the system-level contingency plans are in place so that its cloud-based systems providing critical functions will be available in the event of a disaster.

In recent years, cloud computing has provided a new way for federal agencies to support their business, but fundamental security practices of ensuring adequate security for systems hosted in the cloud remain the same. The belief that the cloud service provider would be

---

[24] DOC, September 2014, *Department of Commerce Information Technology Security Program Policy* (ITSPP), Control CP-2, Washington, DC: DOC.

[25] SaaS is a capability provided to a consumer to use the provider's applications running on a cloud infrastructure. The applications are often accessible via a web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the exception of limited user-specific application configuration settings.

[26] Active Directory (AD) is a directory service created by Microsoft for Windows domain networks. AD provides the means to centrally manage users, workstations, servers, printers, and system information while enforcing security standards. In addition, AD provides the capability to assign access controls to users based on their respective roles.

responsible for everything in the cloud is a serious misunderstanding. While ITA recognized the responsibility of securing its cloud-based systems, it did not make a strong commitment to safeguard its cloud-based systems. Thus, inadequately implementing fundamental security practices, deemphasizing the important roles of its legacy systems, and improperly managing cloud-based systems led to the security deficiencies as illustrated in the findings above.

Recommendations

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, ISSOs, 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.

Summary of Agency Response and OIG Comments

In response to our draft report, ITA concurred with all findings and recommendations, noting that ITA has since remediated a number of the findings. We have included ITA's formal response as appendix C of this report.

Appendix A: Objective, Scope, and Methodology

Our audit objective was to determine whether key security measures are in place to adequately protect ITA systems that utilize cloud computing services.

We reviewed internal security controls significant within the context of our audit objective and employed a comprehensive methodology to validate the security posture of 10 of 19 selected ITA systems. Specifically, we judgmentally selected and reviewed implementation status of fundamental security controls defined in NIST Special Publication 800-53, Rev. 4, including risk assessment, access control, configuration management, identity and authentication, and contingency planning.

To do so, we

- reviewed system-related artifacts, including policy and procedures, planning documents, and other materials;
- interviewed ITA officials, including system owners, the IT security and operations staff, and management;
- analyzed vulnerability scanning results conducted by ITA during FY 2017;
- conducted vulnerability scanning of selected databases and web applications;
- assessed ITA's AWS infrastructure configuration using specialized tools and manual techniques; and
- provided results of vulnerability scanning of selected databases and assessment of AWS infrastructure configuration to ITA for validation and corrective actions.

We reviewed ITA's compliance with the following applicable internal controls, provisions of law, regulation, and mandatory guidance:

- The Federal Information Security Modernization Act of 2014
- U.S. Department of Commerce IT Security Program Policy (ITSPP) and applicable Commerce Information Technology Requirements (CITR):
    - CITR-016, Vulnerability Scanning and Patch Management
    - CITR-019, Risk Management Framework (RMF)
    - CITR-021, Password Management
    - CITR-024, FedRAMP Applicability
- NIST Federal Information Processing Standards Publications (FIPS):
    - FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*

  - FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*

- NIST Special Publications:
  - 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
  - 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
  - 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans*
  - 800-60 Volume I, Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*
  - 800-60 Volume II, Rev. 1, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*

We also used the Center for Internet Security industry best practice security benchmark as criteria for testing cloud-based infrastructure.

We collected computer-generated data created by industry accepted and widely used vulnerability scanning software. We analyzed this data by interviewing knowledgeable ITA officials and providing them the analytical results to eliminate the possibility of false positive results. We determined that the data were sufficiently reliable for the purposes of this report.

We conducted our field work from February 2017 to September 2017 at ITA headquarters in Washington, DC. We performed this audit under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, dated April 26, 2013. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our objectives.

Appendix B: Descriptions of Selected Systems

1. **Antidumping and Countervailing Duty Centralized Electronic Service System (ACCESS)** is the repository for all documents filed in an Antidumping and Countervailing Duty (AD/CVD) proceeding conducted by the U.S. Department of Commerce's business unit Enforcement and Compliance. ACCESS provides the capability for registered E-Filers to submit documents to the record of an AD/CVD proceeding, as well as to search for and view all public documents and public versions. Authorized E-filers may also access business proprietary documents released by Enforcement and Compliance, as appropriate. Registered guest users may search for and view public documents and public versions.
2. **eMenu** provides the capability to find the products or services global markets offices offer, track client participation in events and services, collect any fees, and monitor post/office financial transactions.
3. **Electronic Subsidies Enforcement Library (ESEL)** is a public facing website which provides user-friendly access to information about foreign government subsidy practices.
4. **Free Trade Agreement (FTA) Tariff Tool** hosts information about how U.S. and FTA partner tariffs on individual products are treated under an FTA agreement.
5. **I-92** receives data from Department of Homeland Security's Customs and Border Protection containing I-92 and international flight schedule information, respectively, on a monthly basis. It will import and translate this data into usable data that can be further distributed to clients and the corresponding websites.
6. **ITA Amazon Web Services Platform** provides infrastructure to host multiple ITA systems.
7. **Lotus Notes** provides a broad range of integrated functionality including email, calendaring, instant messaging, forums, blogs, personnel/user directory, and a full office productivity suite.
8. **Microsoft Azure Platform Office 365 (O365)** provides customers with cloud versions of Exchange Online (EXO), SharePoint Online (SPO), and Skype for Business Online (Skype). EXO is an email service. SPO is a solution for creating sites to share documents and information. Skype is a communication service that offers instant messaging, audio and video calling, online meetings, and web conferencing capabilities.
9. **ITA Microsoft SharePoint In Amazon Web Services (AWS)** is an enterprise intranet document management, collaboration, workflow, enterprise search, and internal social networking platform.
10. **Trade Policy Information System (TPIS)** increases public access to U.S. and international trade statistics, provides government analysts with a source of trade information, and provides support for business counseling services. It supports legal and investigative activities related to import protection, export licensing, national security issues, and trade negotiations.

Appendix C: Agency Response

INTERNATIONAL TRADE ADMINISTRATION

March 12, 2018

MEMORANDUM FOR: Frederick J. Meny, Jr.
Principal Assistant Inspector General for Audit and Evaluation (Acting)

FROM: Rand Ruggieri
Acting Chief Information Officer TIMOTHY MCGRAIL Digitally signed by TIMOTHY MCGRAIL Date: 2018.03.13 14:42:47 -04'00'

SUBJECT: FY2017 Federal Information Security Act Audit:
ITA Needs a Stronger Commitment to Safeguard Its Cloud-Based System Draft Report

This memorandum serves as the International Trade Administration's response to the Inspector General's Draft FY2018 Report, ITA Needs a Stronger Commitment to Safeguard Its Cloud-Based System.

ITA's Chief Information Officer concurs with the findings and recommendations outlined in the subject report. The findings accurately reflect the period in which the inspection and testing was conducted. ITA has since remediated a number of the findings and is in the process of documenting our remediation.

ITA notes the challenges of its global users and cloud-based environment. Therefore, continues to make significant investments in cyber security and improvements in its governance procedures and security operations of its cloud-based systems.

ITA OCIO will formally respond to the Recommendations in the near future.

Please contact Angenette Cash, Acting Director, Security Operations and Compliance, at 202-482-6048, if you have any questions.

cc: Sarah Kemp, Acting Deputy Under Secretary, ITA
Rod Turk, Acting Chief Information Officer, DOC
Maria Dumas, Audit Liaison, DOC
Jennifer Eveland, Audit Liaison, ITA

011200000279