



# INTERNATIONAL TRADE ADMINISTRATION

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

FINAL REPORT NO. OIG-12-037-A  
SEPTEMBER 27, 2012

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


**FOR PUBLIC RELEASE**





September 27, 2012

**MEMORANDUM FOR:** Francisco J. Sánchez  
Under Secretary of Commerce for International Trade

**FROM:** Allen Crawley   
Assistant Inspector General for Systems Acquisition  
and IT Security

**SUBJECT:** FY 2012 Federal Information Security Management Act Audit:  
*Improvements are Needed to Strengthen ITA's Information Technology  
Security Program*, Final Report No. OIG-12-037-A

Attached is the final report of our audit of ITA's information security program and practices, which we conducted to meet our obligations under the Federal Information Security Management Act (FISMA). In fiscal year (FY) 2012, we assessed the security of six ITA systems.

We found weaknesses in these ITA systems, including inadequate security categorization that may affect protection of critical bureau 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.

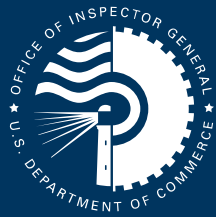
We are pleased that, in response to our draft report, you concurred with our findings and recommendations. We have summarized your response in the report and included the response as an appendix. We will post this report on OIG's website.

In accordance with Department Administrative Order 213-5, please provide us with your action plan within 60 calendar days from the date of this memorandum. The plan should outline actions you propose to take to address each recommendation.

We appreciate the cooperation and courtesies extended to us by your staff during our audit. Please direct any inquiries regarding this report to me at (202) 482-1855 and refer to the report title in all correspondence.

Attachment

cc: Simon Szykman, Chief Information Officer  
Renee Macklin, Chief Information Officer, ITA  
Tim Hurr, Acting Director, Office of Cyber Security  
Jeffrey Jackson, Chief Information Security Officer, ITA  
Justin Guz, Audit Liaison, ITA  
Susan Schultz Searcy, Audit Liaison, Office of the Chief Information Officer



# 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.

# Contents

Introduction .....	1
Findings and Recommendations .....	2
I. Inadequate Security Categorization May Affect Protection of Critical Bureau Information .....	2
II. Security Control Deficiencies Increase the Likelihood of a Successful Cyber Attack.....	3
A. Deficiencies with Vulnerability Scanning and Patch Management .....	3
B. Weaknesses in Securing Databases .....	4
C. Risks Associated with the Presence of Unauthorized Software and Use of Unauthorized Removable Media .....	5
D. Risks Related to Network Implementation .....	6
Conclusion .....	7
<i>Recommendations</i> .....	7
Summary of Agency Response and OIG Comments.....	8
Appendix A: Objectives, Scope, and Methodology.....	9
Appendix B: Agency Response .....	11

*COVER: Detail of fisheries pediment,  
U.S. Department of Commerce headquarters,  
by sculptor James Earle Fraser, 1934*

# Introduction

The strength of the nation's economy continues to depend on global trade, with the United States exporting nearly \$2 trillion worth of goods and services.<sup>1</sup> The International Trade Administration (ITA) plays an important role in improving the global business environment and helping U.S. companies compete at home and abroad through export promotion, commercial diplomacy, shaping industry-specific 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. For example, in November 2011, ITA was notified of a serious cyber attack that had compromised a significant number of its servers, which allowed the attacker to gain full control of ITA's entire enterprise network and access to user account credentials. ITA's investigation of this incident found 66 malicious files residing on its servers and workstations, some present since September 2007. In order to minimize the serious damage caused by this attack, ITA changed all user passwords, consolidated all Internet access through a centralized service, and made architectural changes to its network.

The Federal Information Security Management Act of 2002 (FISMA)<sup>2</sup> requires agencies to secure systems through the use of cost-effective management, operational, and technical controls. The goal is to provide adequate security commensurate with the risk and extent of harm resulting from 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, and the results are 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. See appendix A for details regarding our objective, scope, and methodology.

---

<sup>1</sup> See ITA's *FY 2012–2016 Strategic Plan*.

<sup>2</sup> 44 U.S.C. § 3541 *et seq.* (2002).

# Findings and Recommendations

## I. Inadequate Security Categorization May Affect Protection of Critical Bureau Information

ITA does not have assurance that it has implemented sufficient security controls to protect its information systems, because it has not adequately performed the required step of identifying the critical information in the systems.

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, referred to as *security categorization*,<sup>3</sup> identifies the impact level for a system as high, moderate, or low based on the potential impact to an organization, should an event jeopardize its information and information systems. A system with a higher impact level would require the organization to implement more stringent security controls, compared to one with a lower impact level.

ITA conducted a security categorization for its information and systems, and it determined that all information on its systems is publically available, resulting in an overall rating of moderate for its systems and information. However, we found ITA's analysis to be inadequate; the information security categorization may be at a higher impact level. For example, we identified global trade information collected and processed by ITA that, if compromised, could have severe negative impact to ITA's mission. Specifically, this includes business proprietary information provided by domestic and foreign industries to ITA's Import Administration Antidumping/Countervailing Duty office to initiate and support dumping or illegal subsidies investigations. National Institute of Standards and Technology (NIST) recommends a security categorization of high for such information, which is protected against disclosure by administrative protective orders and other laws. According to senior ITA officials, if this information becomes inadvertently revealed, it could undermine future investigations and the trust businesses place with ITA.

The reason for this inadequate categorization was that ITA did not conduct a comprehensive review of all critical business information on its systems. Instead, ITA based its categorization only on a review of information processed, stored, and transmitted by its e-mail system. By taking this approach, we believe ITA categorized its systems at a lower impact level, thus requiring less stringent security controls.

---

<sup>3</sup> Federal Information Processing Standard (FIPS) 199 provides security categorization guidance for nonnational security systems. National Institute of Standards and Technology, February 2004. *Standards for Security Categorization of Federal Information and Information Systems*, FIPS 199. Gaithersburg, MD: NIST.

## II. Security Control Deficiencies Increase the Likelihood of a Successful Cyber Attack

We identified security vulnerabilities in ITA system components (e.g., servers, workstations, and routers) that increase exposure to cyber attacks and place mission critical data and systems at risk. These weaknesses exist, in part, due to deficient vulnerability scanning and inadequate patch management. Weaknesses further arise due to improperly secured databases. In addition, ITA has unauthorized software on its network and lacks controls to prevent the use of unauthorized Universal Serial Bus (USB) devices,<sup>4</sup> thus opening its systems to additional security risks. Finally, the potential impact of all vulnerabilities identified is significantly greater because of weaknesses in the implementation of ITA's worldwide enterprise network.

### A. Deficiencies with Vulnerability Scanning and Patch Management

ITA's vulnerability scanning of system components and patch management for software products (e.g., Adobe Acrobat, Adobe Flash Player, and Oracle Java) do not effectively identify or remediate security weaknesses. We assessed over 200 system components from ITA's operational systems and found that more than 75 percent of the components had significant vulnerabilities due to missing patches, some available for over 5 years (see figure 1, next page). In fact, attackers could compromise these vulnerable components using known exploits to gain initial unauthorized access, maintain access, and exfiltrate<sup>5</sup> sensitive data. ITA informed us that it could not install some security patches due to legacy applications but planned to address this issue when upgrading the applications.

We did find, however, that ITA has an automated process for patching vulnerabilities associated with Microsoft operating systems and Office desktop productivity software used within its operational systems. In addition, prior to our audit, ITA recognized it had serious deficiencies with patching software products and began developing a process to address this issue. However, improvements are needed to address the following additional deficiencies we found:

- *Deficiencies in server scanning process resulted in ITA servers not being scanned for vulnerabilities. Of the 257 servers in ITA's operational systems, 36 of the servers (14 percent) were not being scanned. This issue resulted from a lack of coordination between ITA's network operations and IT security organizations.*
- *ITA did not scan network routers using administrator-level credentials. Credentialed scans would have allowed the scanning tool to perform a more exhaustive and accurate examination of the routers.*

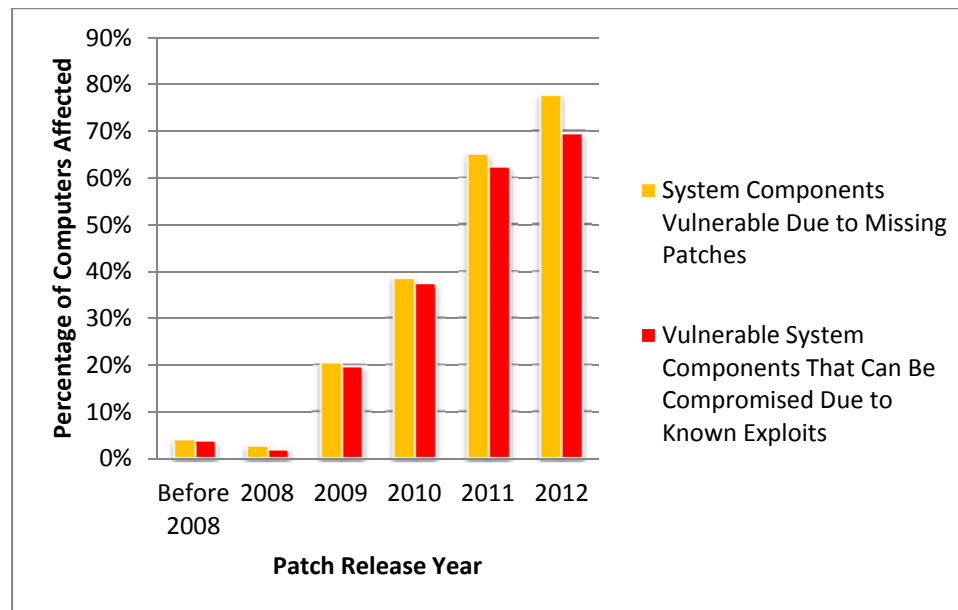
---

<sup>4</sup> *Universal Serial Bus (USB)* is a standard for connecting electronic devices such as thumb drives, MP3 players, and digital cameras, to computers.

<sup>5</sup> *Exfiltrate*, in the context of this report, refers to the unauthorized transfer of sensitive information from an organization to external entities.

- Since July 2011, ITA had not patched servers running virtualized operating systems. Our analysis determined that the vendor had released critical patches for flaws that can potentially allow attackers to gain unauthorized access, and perform denial of service attacks.

**Figure 1. Percentage of ITA System Components Affected By Vulnerabilities, by Patch Release Year**



Source: OIG vulnerability scans and analysis

Note: A system component may have multiple missing patches released in different years.

### B. Weaknesses in Securing Databases

Configuration settings control<sup>6</sup> has been a long-standing FISMA requirement and an essential and fundamental aspect of securing an information system. However, our assessment of ITA's databases revealed serious vulnerabilities. For example, ITA improperly configured one database to use a blank password for authentication to a database administrator account. We validated this vulnerability by successfully gaining access to this account. After further analysis, we determined that an attacker could exploit additional improperly configured database settings to gain access to the underlying operating system, thus obtaining full control of the server. We also identified three additional improperly configured databases that, if exploited, could allow excessive privileges to access sensitive information (e.g., system user passwords).

Adequately implemented configuration settings control has the potential to compensate for other types of vulnerabilities and can limit the impact of cyber attacks. At the time of our fieldwork, ITA was working to implement this control by establishing secure configuration checklists for various IT products, including databases. However, these database checklists did not address critical secure configuration settings that resulted in

<sup>6</sup>Configuration settings control CM-6 is a required control listed in NIST SP 800-53.



these vulnerabilities. ITA needs to establish adequate secure configuration checklists for its databases and then implement them.

**C. Risks Associated with the Presence of Unauthorized Software and Use of Unauthorized Removable Media**

Preventing both the execution of unauthorized software and the use of unauthorized USB devices are key security measures that lessen the risk of a system compromise and the exfiltration of information. Despite ITA's efforts over the last 5 years, it has not effectively protected its systems from such risks.

In 2007, ITA formed an Architecture Review Board (ARB) with the responsibility of approving software for use on its workstations. With this board's approval, ITA maintains a list of authorized software for workstations. However, we found over 150 instances of unauthorized software present on ITA workstations, including music software, browser add-ons such as toolbars, and other software utilities such as hard drive cleaning tools (see table I, below). According to ITA officials, these software products existed because they were installed prior to the ARB's creation.

**Table I. Unauthorized Software on ITA Workstations**

Disapproved Software Type	Number of Computers with Unauthorized Software
Music software	70
Browser add-ons	3
Software utilities	79

Source: results of OIG scan of 117 ITA workstations

Leaving unauthorized software products on ITA workstations can provide opportunities for an attacker to exploit the software's vulnerabilities and, thus, increase the likelihood of successful cyber attacks. After we notified ITA about this issue, ITA took actions to remove the unauthorized software. In addition, ITA is working to expand the ARB's role to approve software used on servers.

In July 2011, ITA deployed a security tool that controls execution of software on its computing components (e.g., workstations and servers). This tool uses a list of acceptable software, known as a *whitelist*, to determine which software it will allow. However, we found that ITA, when deploying this security tool, did not thoroughly examine software residing on its computing components. Because of the large number of software products its employees used, ITA decided to include on its whitelist all of the software present on its computing components. This action inadvertently allowed for the execution of existing software infected with malware, as demonstrated by November 2011 cyber attack. ITA needs to ensure that only authorized software required for its business operations is allowed to execute.

In addition, our assessment identified widespread use of unauthorized USB devices with ITA workstations. Of the 117 user workstations we reviewed in seven regional offices,

we found that 116 (99 percent) have had unauthorized devices connected to them (see table 2, below). Such usage of unauthorized devices can significantly increase the risk of exfiltration of information.

**Table 2. Unauthorized Device Usage with ITA User Workstations**

ITA Regional Office	Number of User Workstations Reviewed	Number of Workstations Having Unauthorized Devices Attached
Beijing, China	44	43
Moscow, Russia	22	22
New York	7	7
Rio De Janeiro, Brazil	9	9
San Francisco	9	9
Singapore	11	11
St. Louis	15	15
<b>Total</b>	<b>117</b>	<b>116</b>

Source: results of OIG scan of 117 user workstations

Department policy<sup>7</sup> does not allow use of such personally owned removal media devices and requires agencies to permit removable media use only when there is a valid business reason. ITA did authorize a specific USB thumb drive for portable storage; however, we found that ITA does not have technical controls in place to ensure that users do not use unauthorized USB devices. ITA is currently working to implement a technical solution to prevent use of unauthorized USB devices.

#### D. Risks Related to Network Implementation

The successful compromise of a computing component within ITA's worldwide enterprise network increases the likelihood that additional components can be compromised. The current implementation of the ITA network allows network traffic to flow freely between all computing components. For example, our testing of ITA's network confirmed that a user's workstation located in Beijing, China, was successfully able to communicate with a development database server located at ITA's main computer center in the United States.

Given the security weaknesses presented in this report, we are concerned that the current ITA network infrastructure could pose a greater security risk on ITA systems and information. Allowing malicious attackers to easily traverse ITA's network increases the risk that the attackers could leverage security weaknesses in one component as a conduit to further attacks against other system components. According to ITA officials, the current network is a legacy design dating back a decade or more. ITA also acknowledged the need to migrate to a more secure network, which includes segmentation of workstations from servers.

<sup>7</sup> DOC CITR-005, Removable Media Devices (December 11, 2008).

## Conclusion

During the past year ITA has undertaken activities to improve its IT security posture. However, unless ITA makes additional improvements to adequately secure its systems, it is likely to encounter additional successful cyber attacks that could seriously harm ITA's mission.

During our audit, we issued two memorandums to ITA's senior management concerning the results of OIG vulnerability scanning. We further briefed ITA staff on our technical assessment results, and they are taking action to correct the deficiencies identified.

## Recommendations

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.

# Summary of Agency Response and OIG Comments

In response to our draft report, ITA concurred with our findings and recommendations. In addition, the agency indicated that it has remediated a majority of the findings and is currently documenting remediation efforts.

# Appendix A: Objectives, Scope, and Methodology

Our objective was to assess the effectiveness of ITA's information security program by determining whether key security measures adequately protect the ITA's systems and its information. Using a combination of automated software tools and manual review, we performed internal and external vulnerability assessments on ITA's systems, including servers, workstations, databases, and network devices. For one system, we limited our scans to the test environment due to the concern that such activity can disrupt the service. We validated that the test system had very similar configurations to the production systems and shared our assessment results with ITA chief information officer (CIO) staff, seeking their feedback to validate identified vulnerabilities to eliminate false positives. We also interviewed business unit officials as needed to understand ITA's business practices and information collected, as well as interface with customers.

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

- FISMA
- IT Security Program Policy, U.S. Department of Commerce, released March 9, 2009
- NIST FIPS publications
  - 199 (Standards for Security Categorization of Federal Information and Information Systems)
  - 200 (Minimum Security Requirements for Federal Information and Information Systems)
- NIST Special Publications
  - 800-37 (Guide for Applying the Risk Management Framework to Federal Information Systems)
  - 800-53 (Recommended Security Controls for Federal Information Systems and Organizations)
  - 800-60 (Guide for Mapping Types of Information and Information Systems to Security Categories)
  - 800-70 (National Checklist Program for IT Products—Guidelines for Checklist Users and Developers)
  - 800-115 (Technical Guide to Information Security Testing and Assessment)

We conducted our fieldwork from January 2012 to May 2012 at ITA Headquarters, Bowie Computer Center, and remotely assessed system components at eight regional offices (Beijing, Mexico City, Moscow, Rio De Janeiro, Singapore, New York, San Francisco, and St. Louis).

OIG performed this audit under the authority of the Inspector General Act of 1978, as amended, and Department Organization Order 10-13, dated August 31, 2006. We conducted this 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.


# Appendix B: Agency Response



UNITED STATES DEPARTMENT OF COMMERCE  
International Trade Administration  
Washington, D.C. 20230

SEP 20 2012

MEMORANDUM FOR: Allen Crawley  
Assistant Inspector General for Systems Acquisition and IT Security

FROM: Renee Macklin   
Chief Information Officer for ITA

SUBJECT: FY2012 Federal Information Security Management Act Audit:  
Improvements are Needed to Strengthen ITA's  
Information Technology Security Program Draft Report

This memorandum serves as the International Trade Administration's response to the Inspector General's Draft FY2012 Report, Improvements are Needed to Strengthen ITA's Information Technology Security Program.

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 majority of the findings and is in the process of documenting our remediation.

ITA notes the challenges of its global users and environment. Therefore ITA continues to make significant investments in IT Security and has hired a new IT Security Team with strong leadership skills and IT Security skills. The team has instituted a vigorous series of testing and remediation protocols, and has expanded the IT Security Team with experts on both the operations and procedural branches. In FY12, ITA made significant progress toward consolidating and improving ITA's infrastructure. However we recognize there is more work that needs to be done and that IT Security remains a continuous improvement process.

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

Please contact Jeffery Jackson, Chief Information Security Officer, at 202-482-5236, if you have any questions.

cc: Ken Hyatt, Acting Deputy Under Secretary, ITA  
Simon Szykman, Chief Information Officer, DOC  
Tim Hurr, Acting Director, Office of Cyber Security, DOC  
Jeffery Jackson, Chief Information Security Officer, ITA  
Justin Guz, Audit Liaison, ITA  
Susan Schultz Searcy, Audit Liaison Office of the Chief Information Officer, DOC



01120000142