

U.S. International Trade Commission

Audit of Hardware Inventory



OIG-AR-15-11

July 22, 2015



Office of Inspector General

The U.S. International Trade Commission is an independent, nonpartisan, quasi-judicial federal agency that provides trade expertise to both the legislative and executive branches of government, determines the impact of imports on U.S. industries, and directs actions against certain unfair trade practices, such as patent, trademark, and copyright infringement. USITC analysts and economists investigate and publish reports on U.S. industries and the global trends that affect them. The agency also maintains and publishes the Harmonized Tariff Schedule of the United States.

Commissioners

Meredith M. Broadbent, Chairman

Dean A. Pinkert, Vice Chairman

Irving Williamson

David S. Johanson

F. Scott Kieff

Rhonda K. Schmidlein



UNITED STATES INTERNATIONAL TRADE COMMISSION

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20436

June 22, 2015

IG-NN-019

Chairman Broadbent:

This memorandum transmits the Office of Inspector General's final report, Audit of Hardware Inventory Management, OIG-AR-15-11.

This audit focused on whether the Commission uses its hardware inventory to manage its network.

In finalizing this report, we analyzed management's comments to our draft report and have included those comments in their entirety as Appendix A. This audit determined that the authorized hardware inventory was effective, and we identified three areas for potential improvement.

This report presents five recommendations to address the areas for improvement. In the next 30 days, please provide me with your management decisions describing the specific actions that you will take to implement each recommendation.

Thank you for the courtesies extended to the auditors during this review.

Philip M. Heneghan

U.S. International Trade Commission

Audit Report

Table of Contents

Results of Audit	1
Areas for Improvement	1
Area for Improvement 1: Populate inventory with appropriate information.	1
Area for Improvement 2: Create a mapping of Ethernet ports to physical locations.	2
Area for Improvement 3: Automated detection of unauthorized hardware.	3
Management Comments and Our Analysis.....	4
Objective, Scope, and Methodology	4
Appendix A: Management Comments on Draft Report.....	A

U.S. International Trade Commission

Audit Report

Results of Audit

The purpose of this audit was to answer the question:

- Does the ITC use its hardware inventory to manage its network?

Yes. The Commission did use its hardware inventory to manage its network.

We found that the Commission effectively used automated tools to create and manage an inventory of authorized hardware, and it reconciled that inventory with the hosts connecting to the network.

The Commission demonstrated that it was able to effectively use its inventory through a monthly reconciliation process to identify unauthorized hosts connected to the network, and was able to remove those detected unauthorized hosts from the network.

Hosts can include physical or virtual servers, laptops, desktops, tablets, printers, network switches, and other connected devices. When they attach to the Commission's network, each of these systems uses at least one Internet Protocol (IP) address, and each detected IP address is referred to as a "host." An effective inventory is necessary to detect all hosts connecting to the network, and reconciliation can identify whether unauthorized hosts are connected, either through the failure of an existing authorization process, or because of someone acting with ill intent to compromise the network.

While the Commission was using the hardware inventory to manage its network, we did identify some areas for improvement, which include: (1) populate inventory with appropriate information, (2) create a mapping of Ethernet ports to physical locations, and (3) develop continuous detection and alerts for unauthorized hardware.

Areas for Improvement

Area for Improvement 1:

Populate inventory with appropriate information.

The Commission's hardware inventory collected several pieces of information to identify detected hosts, identifying their Internet Protocol (IP) address, Domain Name Service (DNS) name, Media Access Control (MAC) address, network adapter manufacturer, and NetBIOS name (typically the name of the computer for Windows-based systems). The Commission has the

U.S. International Trade Commission

Audit Report

ability to populate this inventory with additional information that would be very useful to the audience of this inventory, including such items as property number, serial number, hardware manufacturer, the name of the person or organization responsible for managing this hardware, and the dates the hardware was first detected and last seen on the network.

The OCIO division chief responsible for collecting this data identified another OCIO division chief as the owner for all devices on the network. It would be more useful to the Commission to identify the appropriate persons and/or groups within the Office of CIO responsible for specific equipment. The hardware inventory should contain this specific information to enable the rapid identification and assignment of hardware inventory, management-related tasks to the appropriate party.

The Commission should identify those fields useful to effectively manage its hardware. The Commission should also keep up-to-date with information produced by other relevant Federal entities, including OMB, NIST, DHS, and determine whether that guidance could be useful in its own hardware inventory. The U.S. Computer Emergency Response Team (US-CERT) has developed specific guidance on this subject, linked below:

https://www.us-cert.gov/sites/default/files/cdm_files/HWAM_DataSheet.pdf

Recommendation 1: Populate inventory with descriptive data, including vendor, product, model number, property number, and operating system (OS) version.

Recommendation 2: Populate hardware inventory with the accountable person or organization for each host.

Area for Improvement 2:

Create a mapping of Ethernet ports to physical locations.

The hardware inventory system can be used to identify hosts requiring maintenance or removal from the network. A basic requirement for the Commission to manage its network is to have knowledge of the physical location of the hardware connecting to the network. This information should have been developed as the network was built, and should have been maintained through changes made to the topology.

The Commission did not have a map of this physical connection information. While tools are available that can quickly identify the specific network switch and Ethernet port used to connect to a specific host, the map is necessary to physically locate that host.

U.S. International Trade Commission

Audit Report

In a specific case cited to demonstrate the Commission's ability to identify and remove unauthorized hardware, it was shown that while the Commission was able to disconnect the hardware, it experienced difficulty in physically locating the device. The lack of effort to develop and maintain an accurate hardware map resulted in unnecessary efforts and delays to locate a problematic host.

The Commission should develop and maintain a hardware mapping of its Ethernet ports. The Commission possesses the data to immediately map the majority of ports through its knowledge of the locations of staff workstations and printers. It should require minimal effort to identify any remaining ports.

A developed and updated map would enable the Commission to quickly and easily locate hardware when needed, such as during a security incident when time is of the essence.

Recommendation 3: Develop and maintain a mapping of Ethernet ports to physical locations.

Area for Improvement 3:

Automate detection of unauthorized hardware.

To effectively manage the hardware on the network, the Commission should perform continuous monitoring to detect and identify unauthorized devices connected to its network.

The Commission performs continuous monitoring to scan for devices connected to the network. However, the continuous monitoring program does not automatically alert for the detection of unauthorized hardware. Instead, the Commission relies upon a monthly, manual reconciliation process to identify the presence of unauthorized hardware. The reconciliation process should be automated and performed at least daily.

Because of its monthly reconciliation process, an unauthorized device could connect to the network and remain unidentified for up to a month. A real-time detection and alerting implementation for unauthorized hardware would significantly reduce the length of time this risk poses to the Commission.

Recommendation 4: Deploy automated detection of unauthorized hardware.

Recommendation 5: Deploy automated alerts for detection of unauthorized hardware.

U.S. International Trade Commission

Audit Report

Management Comments and Our Analysis

On July 17, 2015, Chairman Meredith M. Broadbent provided management comments on the draft report. She acknowledged that the Commission had an effective authorized hardware inventory and agreed with our findings on areas for improvement. The Commission plans to make management decisions to address the recommendations in the report.

Objective, Scope, and Methodology

Objective:

Does the ITC use its hardware inventory to manage its network?

Scope:

This audit assessed the management of all physical and virtual hardware connected to the ITC network that had the ability to listen or transmit on the network. This audit assessed the capabilities of the Commission as of June, 2015.

Methodology:

1. Collected inventory from the CIO.
2. Gathered information from appropriate CIO divisions related to their use of the hardware inventory.
3. Analyzed provided inventory and CIO responses, and compared Commission practices to industry and Federal best practices, including guidance from US-CERT.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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 audit objectives.

U.S. International Trade Commission

Audit Report

Appendix A: Management Comments on Draft Report

Chairman



UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

CO84-NN-004

July 14, 2015

MEMORANDUM

TO: Philip M. Heneghan, Inspector General

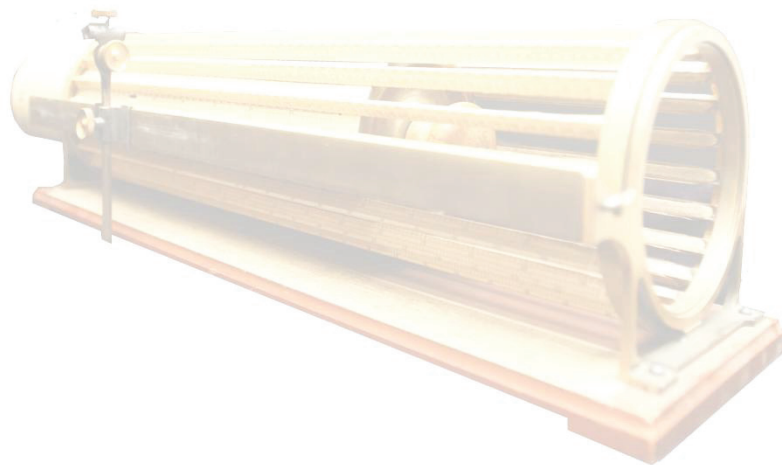
FROM: Meredith M. Broadbent, Chairman *Meredith M. Broadbent*

SUBJECT: Response to the Inspector General's Draft Hardware Inventory Management Audit

I am in receipt of the Inspector General's draft report, *Audit of Hardware Inventory Management*, dated June 22, 2015. I appreciate the opportunity to both review this report and provide comments.

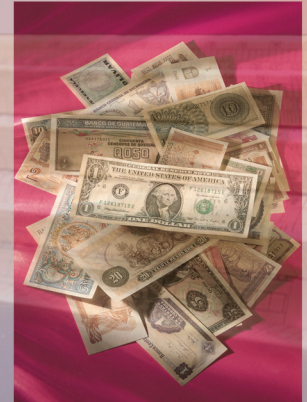
The Inspector General's draft report found that the Commission was effectively using automated tools to create and manage an inventory of authorized hardware on its IT network. While the Commission's management of its hardware inventory was found to be effective, the report also identified areas for improvement. Specifically, the Inspector General recommended that the Commission (1) populate inventory with a more comprehensive set of information (e.g. serial numbers); (2) create a mapping system that will associate ethernet ports to physical locations; and (3) develop continuous detection and alerts for unauthorized hardware.

We agree with the findings and the Commission will institute management decisions that address the recommendations put forth in this report. Thank you for your review.



“Thacher’s Calculating Instrument” developed by Edwin Thacher in the late 1870s. It is a cylindrical, rotating slide rule able to quickly perform complex mathematical calculations involving roots and powers quickly. The instrument was used by architects, engineers, and actuaries as a measuring device.

To Promote and Preserve the Efficiency, Effectiveness, and Integrity of the U.S. International Trade Commission



U.S. International Trade Commission
Office of Inspector General
500 E Street, SW
Washington, DC 20436

Office: 202-205-6542
Fax: 202-205-1859
Hotline: 202-205-6542
OIGHotline@USITC.gov