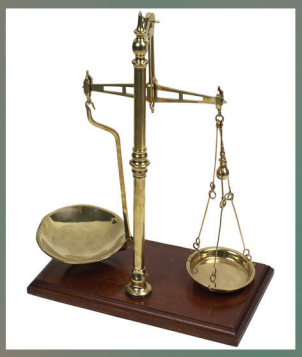
U.S. International Trade Commission

Audit of Software Inventory



OIG-AR-15-12

August 11, 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.

UNITED STATES INTERNATIONAL TRADE COMMISSION

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20436

August 11, 2015 IG-NN-020

Chairman Broadbent:

This memorandum transmits the Office of Inspector General's final report, Audit of Software Inventory Management, OIG-AR-15-12.

This audit focused on whether the Commission uses its software 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 software inventory was ineffective, and we identified two problem areas.

This report presents seven recommendations to address the problem areas. 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

Draft Audit Report

Table of Contents

Results of Audit

The purpose of this audit was to answer the question:

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

No. The Commission did not use its software inventory to manage its network.

In order to manage its network, the Commission should create an authorized software inventory, use tools to identify software installed on the network, and remove unauthorized software. Software can include operating systems, standard installed applications, and executable programs stored on hosts connected to the network.

An effective inventory is necessary to detect software that should not be on the network, either because the authorization process failed, or because someone acted with ill intent to install malicious software, known as 'malware.' While the Commission possessed and used tools related to the inventory and control of software on its network, it did not effectively use these tools. The Commission was unable to manage the software on its network because it did not use an effective software inventory.

During discussions on the results of this audit, a senior staff member with information security responsibility remarked that the Office of Inspector General (OIG) had not given full credit to the Office of the Chief Information Officer (OCIO) for its compensating controls, which he described as sufficient to prevent the installation or execution of malware on the network.

Unfortunately, it is far too easy to disguise malware code to hide its malicious nature from security software. With the exception of whitelisting, a technology implemented to allow only known good software, it is not possible to proactively identify and stop all malware. This is why whitelisting and a software inventory are critical tools in the effort to secure networks.

Concurrent with this audit, the OCIO was undergoing a penetration test. The report described that the testers were able to install and run Mimikatz malware on a computer not protected by whitelisting. This malware revealed domain administrator passwords to give the testers full administrative control of the domain. This action clearly demonstrated that the Commission had no effective means (including security software or monitoring processes) to prevent malware on systems not protected by whitelisting. The report also demonstrated that whitelisting had effectively prevented phishing attempts on systems protected by whitelisting.

We identified the following problem areas in our audit of the Commission's software inventory: (1) no authorized software inventory, and (2) whitelisting not optimally deployed.

Problem Areas

Problem Area 1:

No authorized software inventory.

The CIO provided a software inventory in the form of output from one of its security tools. As presented, this listing provided only software vulnerability information. No information was provided as to whether this software was authorized. The method of collecting this information also resulted in the omission of executable software present but not installed in a standard manner, providing a significant blind spot in the Commission's knowledge of software installed on the network.

It became apparent through discussions of different parties in the office of CIO that different groups had different ideas as to the party responsible for managing a software inventory, and what the capabilities actually were. For example, when asked "How are you alerted to changes in the inventory?" one manager replied with the following: "(whitelisting product) visual alerts, and logs."

Whitelisting is a tool used to block the execution of software on a subset of Commission systems where this software is in operation. Whitelisting provides a visual alert to the person attempting to execute (run) the software, and results in the generation of a log entry. CIO staff could not provide any evidence that staff who managed the software inventory were provided with alerts from whitelisting software. One CIO division was identified as the entity tasked with identifying unauthorized software. When asked how they identified unauthorized software, this group responded "If we come across unauthorized software while researching these threats, vulnerabilities, and network events, then we go through the process to have it removed."

It is not practical or reasonable to manually "come across" and inventory software on a single host, much less an entire network. A review of four types of system executable files on a typical Commission laptop found the presence of 40,728 such files.

Automated tools exist with the capability to enumerate and manage the inventory of installed and otherwise present software applications on the types of systems connected to the Commission's network. The Commission should effectively manage its software inventory through implementation of procedures and automated tools. 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 software 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/SWAM_DataSheet.pdf

Recommendation 1: Develop an inventory of authorized software.

Recommendation 2: Develop a means to detect installed software.

Recommendation 3: Develop a process to reconcile detected and authorized software.

Problem Area 2:

Whitelisting not optimally deployed.

The Commission significantly reduced its software risk through the implementation of whitelisting software for a subset of its systems. This whitelisting software blocks the execution of software not explicitly allowed on systems where it is installed. The Commission could further reduce risk through an optimal deployment of whitelisting. This deployment should include expansion of the technology to the broadest possible number of its networked systems.

The Commission should also correlate the whitelist entries to the authorized software inventory. Currently, the whitelisted software definitions are not reconciled with a listing of authorized software. When a CIO division chief was asked the following, "Please provide the procedure for, and records of manual reconciliations of (whitelisting software) and the Waiver database. How often does this take place? What actions have been taken as a result?" The response received was as follows:

> "If an application is trying to run and failing as a result of (whitelisting), it's verified by the waiver database for approved software. An incident will be created and action taken to address the situation as appropriate (submit waiver, delete/remove, etc.)"

This process fails to account for the possibility that software could be improperly allowed by the whitelist, as a result of improper insertion of software by accident or act of malice, or that software once authorized should no longer be allowed to run on the network.

Once the Commission has created an effective software inventory, it should map its whitelisted software to this inventory, and manage the whitelist by removing entries no longer valid. We have previously recommended the Commission implement whitelisting. We urge the Commission to complete that task.

Recommendation 4: Identify systems that cannot be managed through whitelisting.

Recommendation 5: Deploy whitelisting to all possible systems.

Recommendation 6: Map whitelisted software to authorized software inventory.

Recommendation 7: Implement procedures to remove software whitelist entries when software is no longer authorized.

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 did not have an effective authorized software inventory and agreed with our findings on the problem areas. The Commission plans to make management decisions to address the recommendations in the report.

Objective, Scope and Methodology

Objective:

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

Scope:

This audit assessed the management of software installed on physical and virtual devices connected to the ITC network as of the month of June, 2016. The scope did not include those devices without the ability to install software.

Methodology:

1. Gathered software inventory from the OCIO.
2. Gathered information from CIO divisions related to their use of the software inventory.
3. Analyzed provided inventory and CIO responses, and compared Commission practices to industry and Federal best practices, including guidance from US-CERT.
4. Incorporated results from a security assessment concurrent with the audit.

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.

Appendix A: Management Comments on Draft Report

Chairman

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

C084-NN-003

July 14, 2015

MEMORANDUM

TO: Philip M. Heneghan, Inspector General

FROM: Meredith M. Broadbent, Chairman

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

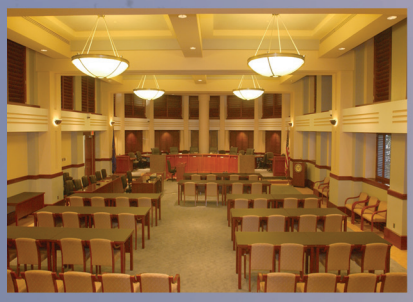
I am in receipt of the Inspector General's draft report, *Audit of Software Inventory Management*, dated June 22, 2015. I appreciate the opportunity to review this report and provide comments.

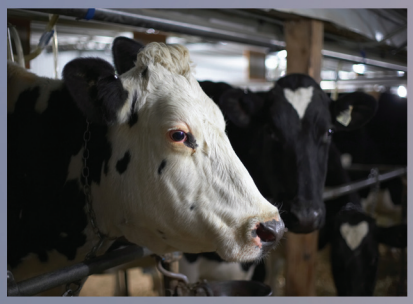
The Inspector General's draft report stated that the Commission did not use its software inventory to manage its IT network. According to the report, this was attributable to the fact that the Commission did not have an authorized software inventory and did not optimally employ its whitelisting capabilities. We agree with the findings and the Commission will institute management decisions that address the recommendations put forth in this draft report.

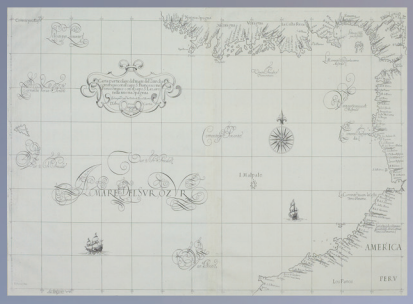
Thank you again for your review.

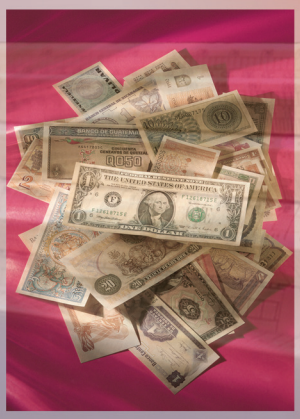
"Thacher's Calculating Instrument" developed by Edwin Thacher in the late 1870s. It is a cylindrical, rotating slide rule able to quickly perform complex mathematical calculations involving roots and powers quickly. The instrument was used by architects, engineers, and actuaries as a measuring device.

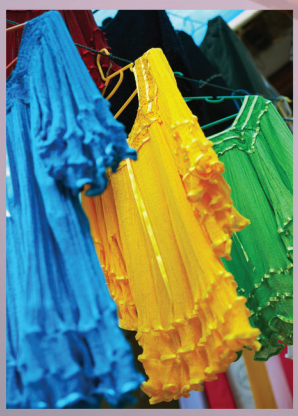
To Promote and Preserve the Efficiency, Effectiveness, and Integrity of the U.S. International Trade Commission











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