U.S. International Trade Commission

Audit of Software Inventory

OIG-AR-10-10

July 13, 2010

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

Deanna Tanner Okun, Chairman
Charlotte R. Lane
Daniel R. Pearson
Shara L. Aranoff
Irving A. Williamson
Dean A. Pinkert

OFFICE OF INSPECTOR GENERAL

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

VIA ELECTRONIC TRANSMISSION

July 13, 2010 OIG-HH-021

Chairman Okun:

This memorandum transmits the Office of Inspector General's final report *Audit of Software Inventory, OIG-AR-10-10*. In finalizing the report, we analyzed management's comments on our draft report and have included those comments in their entirety in Appendix A.

This report contains seven recommendations for corrective action. 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 my staff during this audit.

Sincerely,

Philip M. Heneghan
Inspector General

TABLE OF CONTENTS

Results of Audit **1**

Problem Areas & Recommendations **2**

Problem Area 1: ***Software Is Installed on ITCNet that Is Not Related to Business Needs*** ***2***

Recommendation 1: *That the CIO implement technical controls to prevent users from installing software.* *3*
Recommendation 2: *That the CIO continuously monitor software installed on ITCNet.* *3*
Recommendation 3: *That the CIO implement a process to identify and remove unapproved software.* *3*

Problem Area 2: ***The Commission Uses Multiple Applications to Perform the Same Function*** ***3***

Recommendation 4: *That the CIO set up a process for business users to establish a list of USITC's approved applications.* *4*

Problem Area 3: ***Software Versions are Not Standardized*** ***4***

Recommendation 5: *That the CIO implement a software standard that specifies the versions of software in use on ITCNet.* *5*
Recommendation 6: *That the CIO establish a process to deploy upgrades to all systems on the network unless a specific exception is made for business reasons.* *5*
Recommendation 7: *That the CIO remove all software not supported by its manufacturer.* *5*

Management Comments and Our Analysis **5**

Objective, Scope, and Methodology **6**

Appendix A: Management Comments on Draft Report

Results of Audit

The purpose of this audit was to answer the question:

> Is the Office of the CIO maintaining an accurate inventory of software on ITCNet?

We found that the Office of the CIO does not maintain an accurate inventory of software on ITCNet.

Our inventory of ITCNET workstations during the month of May, 2010, identified the following:

- Installations of software such as games, screensavers, and chat software
- One workstation has 211 applications installed, including iTunes, Big Fish Games, and TurboTax
- Eight software packages from different vendors for working with PDF files
- Five major versions of Adobe Acrobat (and many more minor versions)

The Office of the CIO provided a listing of 26 "Standard Applications," and a listing titled "Software Inventory" which included 234 applications. Combined, these lists total a maximum of 260 inventoried software applications. However, we identified more than one thousand unique installed applications on ITCNET.

An analysis of the installed applications identified software not related to business needs; the use of multiple applications from different vendors to perform the same function; and installations of multiple major and minor versions of the same application. This report details these problem areas, and provides recommendations to resolve these issues.

Problem Areas & Recommendations

Problem Area 1:
Software Is Installed on ITCNet that Is Not Related to Business Needs

A review of the USITC's workstation software inventory identified several types of software unrelated to business needs, including the following:

- Games and Screensavers, including:
  - Monopoly
  - Truck Dismount
  - Elf Bowling 7 - The Last Insult
  - Big Fish games
- Chat software, including:
  - GAIM
  - Pidgin
  - Yahoo messenger
  - Skype
- Miscellaneous software, including:
  - TurboTax
  - DietMaster2000
  - MTV Networks URGE
  - Folding@home/Fold-It
  - NetFlix Movie Viewer

Workstations at the Commission provide a standard suite of software, including applications such as Microsoft Office, Word Perfect Office, and Adobe Acrobat. Some staff have unique business needs, and require access to additional applications. One such example is SAS, which is used by Commission economists.

According to current policy, requests for non-standard software require supervisory and CIO approval. This policy is not being consistently followed, and there are inconsistent or ineffective technical controls to prevent users from installing software and bypassing the approval process.

As of May 28, 2010, 130 users, or roughly one-quarter of all ITC staff have administrative privileges. In order to run certain legacy software, administrative privileges are required. As the standard workstation configuration does not provide these privileges to a standard user, users with this requirement have been provided

administrative privileges on their workstations. However, an unintended side effect is that these elevated credentials also grant users the technical ability to install software of their choice. In addition to allowing users to intentionally install software, this capability can be exploited by malicious email or Internet sites to covertly install software that compromises the security, integrity, and availability of Commission data.

Because it does not control the software being installed on its network, the Commission does not know whether all software on ITCNet is safe or properly licensed.

Effective software inventory management practices will reduce support requirements, limit vulnerabilities, and provide a better means of complying with software licensing requirements.

Recommendation 1:

That the CIO implement technical controls to prevent users from installing software.

Recommendation 2:

That the CIO continuously monitor software installed on ITCNet.

Recommendation 3:

That the CIO implement a process to identify and remove unapproved software.

Problem Area 2:
The Commission Uses Multiple Applications to Perform the Same Function

Adobe Acrobat is installed on virtually every ITCNet workstation, and is used to work with PDF (Portable Document Format) files. Despite the universal presence of Adobe Acrobat, we found seven additional applications that perform the same function:

- Aquaforest Autobahn DX,
- Acro Software CutePDF,
- Foxit Reader,
- Software995 PDF995,
- SkySof PDF Maker,
- EXP Systems PDF reDirect, and
- VeryPDF DocConverter.

This condition is not unique to PDF applications. Additional examples from ITCNet include four Internet Browsers: Internet Explorer, Apple Safari, Google Chrome, and Mozilla Firefox; and three file compression utilities: 7zip, WinRAR, and WinZip.

The Commission should select an application that performs a business function well, and then all users with that business need should use only that application. Business functions should be performed with the minimum possible number of software applications. It may not be possible in all circumstances to select a single application, but the installation of different software performing similar functions should be an exception rather than the rule.

No process exists to require business users to select from a listing of approved, standard applications. Business users must be made aware that the cost to implement and support software greatly exceeds the purchase price in an enterprise environment. Unnecessary installation of multiple brands of software providing similar functionality results in an increase in both support costs and exposure to risk.

Recommendation 4:

That the CIO set up a process for business users to establish a list of USITC's approved applications.

Problem Area 3:
Software Versions are Not Standardized

We identified many instances of different major and minor versions of the same software installed on ITCNet. For example, Word Perfect Office exists at versions X3, X4, and X5; Internet browsing software Mozilla Firefox is installed in three major versions, 2.0, 3.0, and 3.5, and 14 different minor versions; and Adobe Acrobat versions included 5.0-5.05, 6.0.2, 7.0.0-7.1.0, 8.0.0-8.2.2, and 9.0.0-9.3.2.

Version differences for identical software should be limited to allow the network to be managed efficiently. Using multiple versions of applications increases the level of effort required to maintain and support software by Help Desk staff. For example, applying security patches to an application requires a specific level of effort. If a patch affects both Adobe Acrobat versions 8.0 and 9.0, double the effort is required to distribute this patch. The workload required to apply security patches would be significantly reduced by limiting applications to one installed version.

When new major software versions are released, vendors typically set a sunset date for support of older versions. Once this date is reached, the vendor stops providing fixes for this older software. For example, Adobe Acrobat versions 5.0 and 6.0 are installed on the network, but are no longer supported by their manufacturer. These versions of the software are beyond the sunset date, and have vulnerabilities that cannot be patched. To maintain the security of its network, the CIO should remove unsupported software from ITCNet.

The Commission does not have a business process to determine when to upgrade or remove software across the network. When a newer version of software is released, the Commission should implement a plan to perform an upgrade of all ITCNet workstations and remove all legacy versions of the software.

Recommendation 5:

That the CIO implement a software standard that specifies the versions of software in use on ITCNet.

Recommendation 6:

That the CIO establish a process to deploy upgrades to all systems on the network unless a specific exception is made for business reasons.

Recommendation 7:

That the CIO remove all software not supported by its manufacturer.

Management Comments and Our Analysis

On July 6, 2010, Chairman Deanna Tanner Okun provided management comments to the draft audit report. The Chairman agreed with our assessment that the Commission has not maintained an accurate and full accounting of installed software applications, and recognized the need to resolve the three identified problem areas.

Objective, Scope, and Methodology

Objective:

The objective of the audit was to answer the question, "Is the Office of the CIO maintaining an accurate inventory of software on ITCNet?"

Scope:

This audit was performed against all workstations on ITCNet, and included operating systems as well as major and minor applications.

Methodology:

- We performed a software inventory of ITCNet using Spiceworks v. 4.7.50804 configured with credentials granting access to all workstations.
- We analyzed the Spiceworks generated data with Microsoft Access and Excel to identify categories of applications, versions in use, and the number of installations.
- We collected the number of administrative users by parsing data generated by Nessus workstation scans.
- We verified the data by comparing it to software installed on workstations.
- We conducted interviews with CIO staff
- We received documentation to support information received in interviews.

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

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436
CO76-HH-004

July 6, 2010

MEMORANDUM

TO: Philip M. Heneghan, Inspector General

FROM: Chairman Deanna Tanner Okun

SUBJECT: Management Response to the Inspector General's Draft Audit Report, "Audit of Software Inventory"

I am in receipt of the Inspector General's draft report, *Audit of Software Inventory (IT-002)*, dated June 7, 2010. I appreciate the opportunity to review the draft report and to provide a response to the findings.

The Inspector General's draft report addressed the question of whether the Commission maintains an accurate inventory of software on ITCNet. You identified three problem areas that require immediate agency action. I concur with your assessment of these problem areas. Management of the Commission's network environment and resources is a critical task and as you found, the agency has not maintained an accurate and full accounting of installed software applications. As the Commission has noted previously, we take seriously the importance of protecting our data and systems from possible attacks and other risks. Measuring, assessing, managing, and reducing risks associated with the desktop computing environment are priorities for the Commission.

The Commission has undertaken a number of immediate corrective actions in response to the draft audit report. In conjunction with efforts undertaken to address your findings in your earlier audit on the patching of ITCNet workstations, all agency desktops and laptops have been reconfigured to a standard image of 18 software applications. Any non-standard software will be approved only through a waiver request. In addition, the number of employees who hold local

administrative rights over their local desktop environment will be limited to those who submit a waiver to the CIO that demonstrates a need for those rights.

I address each particular finding below.

1. Software is Installed on ITCNet that Is Not Related to Business Needs

I concur with the audit's findings that despite agency policy that requires supervisory and CIO approval for non-standard software, this policy was not consistently followed and controls were not in place to prevent individual users from installing software outside the approval process. The Office of the CIO will be instructed to put in place a comprehensive program to manage its software inventory, and thus limit potential security vulnerabilities and ensure that all software installed meets a business requirement and is properly licensed.

2. The Commission Uses Multiple Applications to perform the Same Function

I agree with the audit's finding that running multiple applications to perform similar functions can increase the Commission's support costs and exposure to security risks. I will instruct the CIO to review requests for applications beyond the standard image installed on individual workstations and work to improve the process through which the CIO approves exceptions to this rule by requiring recertification of waiver requests on an annual basis.

3. Software Versions are Not Standardized

I agree that to maintain an accurate software inventory and allow the most efficient and effective security posture for ITCNet, the CIO should set a goal to limit software applications to a single version, and remove from the network software that is no longer supported by the vendor. The CIO will develop a process to monitor exceptions that have been granted through the waiver process, and review at least on an annual basis the continuing need for legacy versions of software.

"Thacher's Calculating Instrument" developed by Edwin Thacher in the late 1870s. It is a cylindrical, rotating slide rule able to 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: 202-205-2210
Fax: 202-205-1859
Hotline: 877-358-8530
OIGHotline@USITC.gov