U.S. International Trade Commission

Audit on the Patching of ITCNet Workstations

OIG-AR-09-10 **June 23, 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.

OFFICE OF INSPECTOR GENERAL

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

VIA ELECTRONIC TRANSMISSION

June 23, 2010 OIG-HH-017

Chairman Okun:

This memorandum transmits the Office of Inspector General's final report *Audit on the Patching of ITCNet Workstations, OIG-AR-09-10*. 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 six 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

The purpose of this audit was to determine whether the process for patching ITCNet workstations is materially and effectively reducing the Commission's risk.

The process for patching ITCNet workstations is ineffective and exposes the Commission's information and systems to material risk. On April 28, 2010 we reviewed the patch status of 354 machines on ITCNet and found that:

- All workstations were missing High Severity patches—a High Severity patch is a software change designed to prevent intruders from being able to run code of their choice on our network or elevating their privileges to take control of ITCNet workstations
- 28,320 High Severity patches were missing on ITCNet workstations
- An average of 80 High Severity patches were missing per workstation
- 236 workstations were missing a High Severity Microsoft Outlook patch that has been available since January 10, 2006,
- 308 workstations were missing High Severity Java patches
- 307 workstations were missing High Severity Adobe Acrobat patches
- 253 workstations were missing High Severity Flash Player patches

The patching process for workstations on ITCNet is ineffective because the Office of the CIO does not measure its patch status; responsibility for patching is unclear; and there is no automated process to patch all workstations. Each of these three problem areas will be discussed in detail in the rest of this report.

Problem Areas & Recommendations

Problem Area 1:
The Commission Does Not Measure the Patch Status of Workstations

The Office of the CIO is not monitoring the patch status of ITCNet workstations. This lack of monitoring is partially responsible for the fact that workstations are not being patched. Our analysis of 354 workstations determined that High Severity patches were missing from every machine tested. On average, each system was missing 80 High severity patches.

Effective management is only possible with consistent measurement. Because the Office of the CIO is not measuring the patch status of workstations, it is not managing the workstation patching process.

Not patching workstations on our network exposes more than just a single computer to risk, rather it exposes all data and systems on ITCNet to risk. For example, the administration of applications such as EDIS, HTS, and DataWeb require that staff use elevated credentials. Administration of these applications takes place on user workstations. When a workstation is compromised, the attacker gains control of that workstation and receives access to the elevated credentials in use on that workstation. All that is required for complete compromise of any application being used at USITC is for an attacker to exploit only one of the average 80 missing High Severity patches on any workstation in use by an application administrator. This weak link effectively circumvents the other security applied to the network perimeter or the application itself.

Senior management in the Commission's business units are not aware of the risks to the confidentiality, integrity, and availability of data on their information systems because they are not regularly informed of the status of workstation security.

Recommendation 1:

We recommend that the CIO deploy a tool to measure the patch status of workstations on ITCNet.

Recommendation 2:

We recommend that the CIO report monthly on patch status of workstations to all senior management in the Commission.

Problem Area 2:
The Responsibility for Patching Workstations is Unclear

Our review of the workstations on ITCNet found that the Commission was missing a total of 28,320 High Severity patches on its workstations. Every workstation we tested was found to be missing Microsoft patches.

Third party software such as Java, Acrobat, and Flash Player are installed on every workstation. If this software is not patched, it creates another attack vector. We did not find any evidence that this third party software is being consistently patched. We identified 308 workstations missing High Severity Java patches, 307 missing High Severity Adobe Acrobat patches, and 253 missing High Severity Flash Player patches.

During our interviews with OCIO staff, we learned that the Office of the CIO expects Commission staff to patch applications outside the scope of the CIO software baseline.

In interviews with non-OCIO users that had third party software installed on their workstations, we asked "Who patches your software?" We received the following types of responses:

- "What's patching?"
- "I don't patch it."
- "Sometimes, it pops up a message about downloading a newer version, and I always click 'No'."
- "Doesn't the CIO take care of all patching?"

Commission users are unaware that the OCIO doesn't patch all of their software. While users should be aware of the inherent risks of Internet browsing and email attachments, expecting every user to implement technical mitigations creates a significant risk to all ITCNet users.

We also noted that unauthorized software was running on ITCNet, and was not being patched. For example, Apple iTunes was running on 19 workstations and High Severity iTunes patches were missing from all 19 of these workstations.

In order to effectively manage the patching process, a single individual should have the authority and responsibility to patch ITCNet workstations.

The effects of the unclear roles (between the OCIO and users) are that workstations are not patched and that the Commission information systems are vulnerable, and operate under a high level of risk.

Recommendation 3:

We recommend that the CIO assign the authority and responsibility to one individual to maintain patches on all workstations on ITCNet.

Recommendation 4:

We recommend that the CIO implement processes to manage the patching of software approved by waiver.

Recommendation 5:

We recommend that the CIO set up a process to remove unapproved software from ITCNet.

Problem Area 3:
There is No System-wide, Automated Process for Patching Workstations

Our review of the patch status on workstations identified many instances of common standard applications that have remained unpatched for years. For example, we found that a High Severity patch released January 10, 2006 for Microsoft Outlook (MS-06-003) was missing from 236 workstations. This software is part of the OCIO software baseline, and by policy, should be patched by the OCIO.

High Severity patches for all software should be applied agency-wide within 3 days of release by their manufacturer. High Severity patches should be installed for most systems on the same day a patch is released, because exploits are generated quickly from the information provided as part of the patch. Any delay beyond the release date of a patch increases the risk exposure. For this reason, Microsoft preconfigures Windows operating systems to download and install patches every night.

We identified one system missing 297 High Severity patches.

Commission staff should be protected from malicious content encountered while browsing the Internet or received via email. Unpatched workstations are missing these basic protections, and greatly increase the risk of system compromise.

The Commission's current patching method demands significant resources because it is not fully automated. Because it does not immediately apply all necessary High Severity patches, the Commission is operating under a high level of risk. As a result, the Commission does not have the most basic defenses to secure its workstations and its network. The current patching process does not effectively protect Commission information or systems.

Recommendation 6:

We recommend that the CIO implement an automated patching process of all workstations on ITCNet.

Management Comments and Our Analysis

On June 16, 2010, Chairman Shara L. Aranoff provided management comments to the draft audit report. The Chairman concurred with our assessment, and acknowledged that the three problem areas highlighted present significant material risks.

Based on the information obtained during the course of this audit, the Commission undertook immediate action to reduce its vulnerabilities through the replacement of most workstations with a new, fully patched workstation.

In her comments, the Chairman reports that as of June 16, 2010, the aggregate number of missing High Severity patches had decreased by 91.7%, from 28,320 to 2,333, and that the number of systems fully patched had increased from 0 to 197 workstations.

We have continued to monitor the patch status since the original assessment, and our data confirms a significant decrease in the number of missing patches and an increase in the number of fully patched workstations. As of June 16, 2010, the average number of missing High Severity patches per workstation has decreased from 80 to 7, as seen in Chart 1. When our testing began, no workstations were fully patched; Chart 2 details the increase of fully patched workstations to 61%.

Chart 1: Average Missing High Severity Patches.

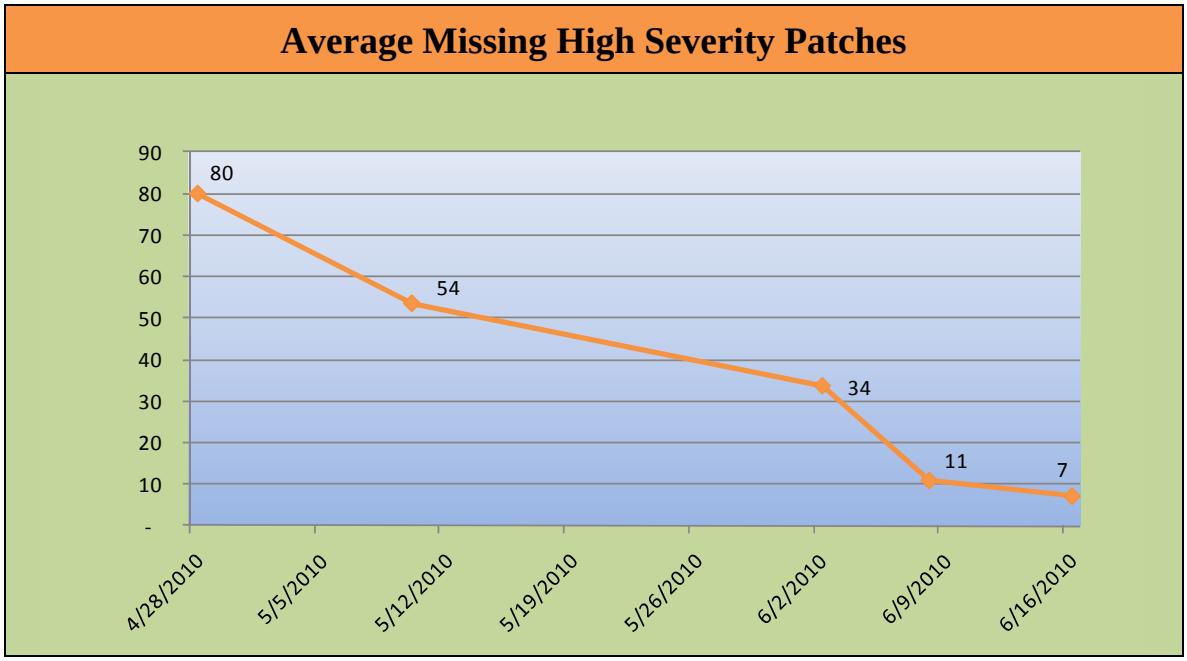
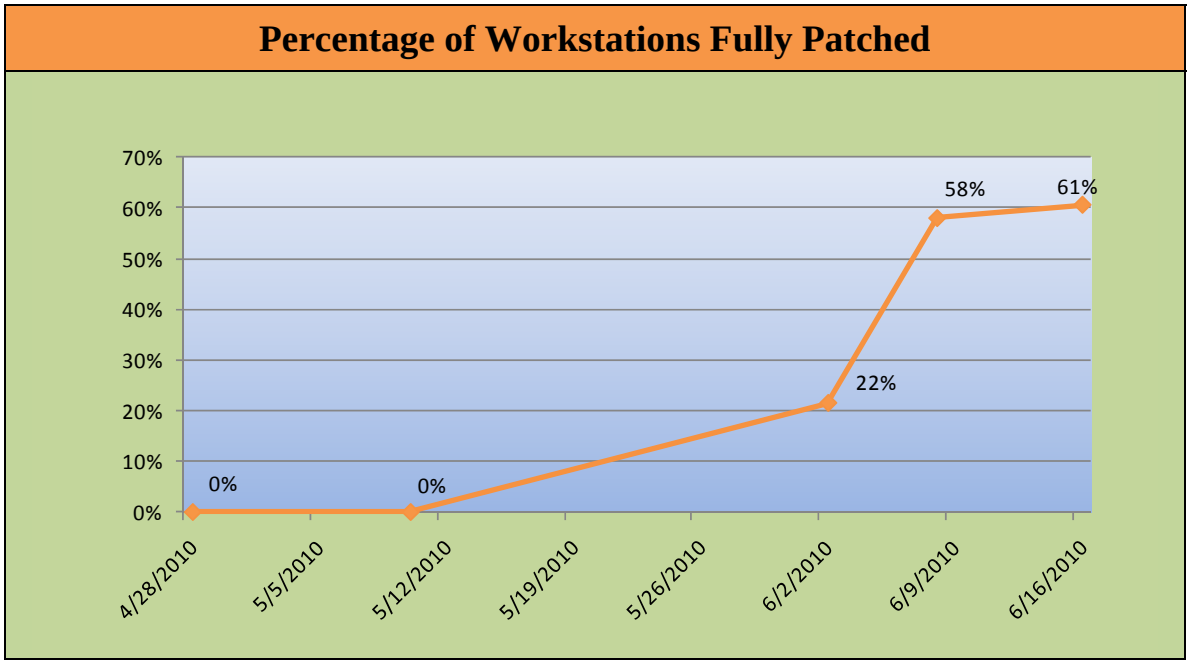


Chart 2: Percentage of Workstations Fully Patched:



Objective, Scope, and Methodology

Objective
The objective of the audit was to answer the question, "Is the process for patching ITCNet workstations materially and effectively reducing the Commission's risk?"

Scope
The original scope of this audit was intended to provide a comprehensive view of ITCNet to include all nodes, including servers, security and network infrastructure, and all other addressable devices. After discussions with the OCIO we reduced the scope to focus only on workstations.

This audit covered all workstations on ITCNet and all software on these workstations, including operating systems and both major and minor applications. In addition, it evaluated the recommended patch status of the software installed on each machine.

On April 28, 2010, we assessed the patch status of all workstations residing in the standard ITCNet workstation network range.

Methodology
A combination of automated tools, manual validity checks, and interviews with USITC staff were used to gather and analyze information in order to determine the state of the Commission's patching process.

a. To analyze the patch status of the workstations on ITCNet, we first identified which networks on ITCNet hosted workstations. To perform this task, we queried CIO staff, and performed passive network and device discovery using Wireshark.
b. To assess the patch status, we used Nessus, which we connected to each workstation with credentials that permitted read access to the areas required to make the assessment, administrative shares and the Windows Registry. While Nessus has the ability to report on a wide range and severity of vulnerabilities, we reported only on High Severity vulnerabilities, which can be used maliciously by intruders to run code of their choice on our network or to elevate privileges to take control of our workstations.
c. To limit the risk inherent in scanning tools, we first scanned workstations and non-workstations (printers) in the Office of Inspector General. After we validated the results with manual checks, we scanned about ten percent of the workstations on ITCNet. We validated those results and then on April 28, 2010 we scanned all known ITCNet network ranges.
d. We confirmed the results generated by Nessus through manual, independent verification of affected file versions on user workstations.
e. After analyzing the results, we conducted interviews with OCIO staff to gather information on the potential causes.
f. We evaluated the current patching process, specifically focusing on installation procedures and patch-level assessment performed by the Office of the CIO.
g. We interviewed non-CIO staff to gather knowledge of their understanding and responsibility in the patching process.

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
CO80-HH-008

June 16, 2010

MEMORANDUM

TO: Philip M. Heneghan, Inspector General

FROM: Chairman Shara L. Aranoff

SUBJECT: Management Response to the Inspector General's Draft Audit Report, "Audit on the Patching of ITCNet Workstations"

I am in receipt of the Inspector General's draft report, *Audit on Patching of ITCNet Workstations* ("ITCNet Report"), dated May 17, 2010. I appreciate the opportunity to review the draft report and to provide a response to the findings.

The Inspector General's draft report on the patching of ITCNet workstations identifies three problem areas that require immediate attention. I concur with your assessment and acknowledge that each of the three problem areas highlighted in your report presents significant material risks to the agency's information and systems. While the existence of these vulnerabilities is unfortunate, I appreciate the fact that your office has identified them. The Commission takes seriously the importance of protecting its 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. As of June 7, all agency desktops and laptops, with the exception of developer workstations in the Office of CIO and modeler workstations in Office of Economics, have been replaced with reimaged machines containing fully-patched system and application software. These two exceptions are due to the highly specialized nature of the configurations; the affected machines will be brought up to latest patch levels by June 30. Vulnerability scans performed by

the Office of the IG on June 16 show a reduction in the number of high vulnerabilities across the enterprise to 2,333, a 91.7 percent decrease from the original number of vulnerabilities identified. The scan also showed that 197 of 325 workstations were fully patched. Going forward, the CIO is evaluating a commercial tool that, if proven effective, will help significantly to maintain patch levels according to the Commission's written patching policy.

I address each particular finding below.

1. The Commission Does Not Measure the Patch Status of Workstations

While the Commission has undertaken efforts to identify vulnerabilities in our computing environment, the actions taken to address the vulnerabilities on our workstations have not been successful. The Office of the CIO will be instructed to develop a comprehensive workstation patching process that will employ the most appropriate tools available to measure patch status and apply critical patches on a regular basis, to reduce to the greatest extent possible the security risks now inherent in the agency's processes and systems.

2. The Responsibility for Patching Workstations is Unclear

While the responsibility for patching the Commission's workstations has been unclear we are now making it clear that the security of ITCNet, including patching, is the responsibility of the Office of the CIO and not the individual users of the workstations. The CIO will be directed to assign an employee currently on staff to be responsible for the measurement and management of the patching process, and to report on a regular basis to the CIO and the Commission as to the patch status. The CIO will continue to provide awareness training to users as a first line of defense; however, the responsibility to patch software and remove unapproved software will be the CIO's responsibility.

3. There is No System-Wide Automated Process for Patching Workstations

I concur that the lack of an automated process for patching workstations opens the agency's system to be compromised. The Office of the CIO is undertaking an immediate action to upgrade or refresh every workstation in the agency in order to strengthen the security and risk posture. A fully patched standard desktop image is being applied to all machines, which will reduce our immediate problem and establish a secure baseline on which an appropriately automated process can be built.

“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