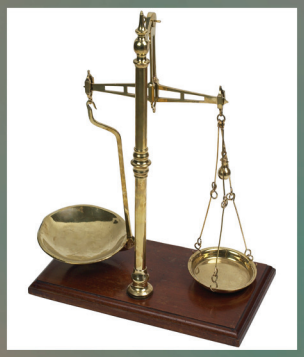
U.S. International Trade Commission

Audit of Log Management



OIG-AR-11-10

April 28, 2011

UNITED STATES INTERNATIONAL TRADE COMMISSION

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

April 28, 2011 OIG-JJ-006

Chairman Okun:

This memorandum transmits the Office of Inspector General's final report Audit of Log Management OIG-AR-11-10. 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 three 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 objective of this audit was to determine:

> Are system logs configured and monitored in a way that adds value to the operation of ITCNet?

No, the ITC has not configured its systems logs in a way that adds value to the operation of ITCNet.

Network devices such as workstations, servers, and firewalls create logs listing information about operational actions as they occur. This information can include the who, what, when, where, why, and how of the following types of data:

- Success or failure of login attempts;
- Permission changes;
- Unusual system loads;
- Resource access (suspicious and otherwise);
- Changes in system performance; and
- System and application errors.

The hundreds of devices on ITCNet can potentially generate millions of logged events per day, requiring the use of an automated program to collect, analyze, and efficiently distribute this data to the groups responsible for managing these systems. If the logged data does not get to the right people at the right time—logging is of limited value.

A log management program adds the most value by collecting log data from all infrastructure devices, including firewalls, application servers, authentication devices, and network equipment. This program would be designed from the ground up with input from multiple groups, including server operations, network management, database and application administrators, desktop support, network security administrators, and IT management. The program would monitor for both minor and severe incidents, storing aggregate data on each, and report instantly to the respective responsible groups for immediate corrective action. These groups would maintain access to the tools available in this program so that reports can be run on demand in order to gain an understanding of current and historical activity.

ITC currently has numerous tools in place to collect and analyze logs. One tool collects data about network traffic, analyzes this data to detect intrusions, and reports this information to one network security engineer. Another tool collects data from workstations, firewalls, the core switch, and a couple of servers, and reports this data to another network security specialist. Still more tools exist that collect performance metrics system status from a collection of servers and the core switch, reporting this data to different operational staff.

ITC possesses a number of tools, but it lacks a coherent log management program with a comprehensive view of logs from all servers, security, and network devices, that provides useful and timely information to all operational groups responsible for the upkeep of ITC's systems.

During the course of this audit, we identified three problem areas. First, the Commission's Security Information and Event Management tool has not been configured to monitor the whole of ITCNet infrastructure, greatly limiting its value. Second, although this tool is configured to monitor workstations, information being gathered by the tool is not being reported to operational staff, further reducing the value of its implementation. Finally, the clocks on all ITCNet devices are not synchronized, making it difficult to correlate events affecting multiple devices.

Problem Areas

Problem Area 1:
Server, network, and security infrastructure is not being centrally monitored with the Commission's designated Log Management tool.

The USITC invested in a Security Information and Event Management tool to perform automated log collection, analysis, and reporting of events network-wide on ITCNet. With the exception of two servers, at the time of the audit the system was only shown to be monitoring workstations on ITCNet, and was not configured to monitor the whole of the server, network, and security infrastructure.

Networked computer devices are capable of producing detailed logs of system activity. Depending on the capabilities of each device, these logs can record tens of thousands of events per day, making it impossible for a human to read, much less analyze, these events. For this reason, organizations implement automated systems to capture, analyze, and report on this log data.

ITC will not be fully aware of events happening across its server, security, and network infrastructure until its SIEM tool is configured to effectively monitor all devices in the ITCNet infrastructure.

Recommendation 1:

Fully configure the Security Information and Event Management (*SIEM) tool to monitor all ITCNet infrastructure.*

Problem Area 2:
Log data is not being effectively used.

The output of an effective log management system is the communication of useful information to responsible parties. On ITCNet, we found repeated errors being logged on every workstation we examined. An effective log management system would have identified and reported this as a problem for resolution by operational staff.

All devices on the USITC network are capable of generating logs of events. These logs can identify a range of events, including configuration changes, hacking attempts, and misconfigured software.

All USITC workstations running Microsoft Windows XP maintain an Application event log that stores event data related to applications. Anyone can view this log by performing the following steps:

1. Right-click "My Computer";
2. Click "Manage";
3. On the left side, click "Event Viewer";
4. Double-click "Application" in the right pane; and
5. The pane changes to show a number of events regarding applications on the PC.

In one example, over a 24 hour span, a single workstation logged 122 errors with the source of "crypt32", with two different messages as follows:

- Failed extract of third-party root list from auto update cab at: <http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab> with error: A required certificate is not within its validity period when verifying against the current system clock or the timestamp in the signed file; and

- Failed auto update retrieval of third-party root list sequence number from: <http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt> with error: This network connection does not exist.

The severity and impact of logged events vary. These specific errors indicate that the workstation is misconfigured for ITC's network, and is repeatedly trying and failing to perform a specific operation. In this case, users are most likely not impacted by this error, but this type of event ends up filling the logs, making it more difficult to find other more pertinent events when troubleshooting system problems. A review of two other workstations online since last year found the following errors related to crypt32:

- Workstation 1: 54,482 of 61,226 (89%) total events between 5/28/2010 and 3/4/2011 (195 per day); and
- Workstation 2: 78,645 of 86,521 (91%) total events between 6/2/2010 and 3/4/2011 (286 per day).

A simple configuration change is all that is required to resolve the cause of these errors and to stop the clogging of workstation Application logs. An effective log management program would report that an event is occurring as often as 80,000 times per day across ITC's 400 workstations, and this information could then be used to prioritize resources for resolving such common and easily solved problems.

The log management program is not effectively reporting common system errors to responsible operational groups, resulting in the delayed resolution of system errors.

Recommendation 2:

Configure the SIEM tool to provide reporting to groups responsible for the operations of workstations, applications, databases, servers, security, and network management.

Problem Area 3:
Clock synchronization is not fully implemented on ITCNet.

In a review of 10 ITCNet devices, we found that the clocks of half of them were not synchronized.

To understand and correlate the events taking place on a network, it is more important to have a consistent "ITCNet time" than the "correct time," (but these are not mutually exclusive). All network devices maintain a system clock, which is used as a timestamp when logging events on that device. This synchronized system clock is a core requirement for network analysis and forensics. In order to correlate an incident that affects multiple systems, clocks on all systems must have the same time.

To maintain clock synchronization on a network, two things are required:

1. A central time server; and
2. Configuration of each device to set its time to that central time server using Network Time Protocol (NTP).

ITCNet does have a central time server, and some systems are synchronizing their clocks with this server. Visible evidence of this is that the clocks are synchronized across two

completely different systems: workstations and desk phones, both of which synchronize with the central time server.

In our survey of 10 infrastructure devices, including servers, switches, routers, and firewalls, only five were found to share the same time. The five devices that didn't have "ITCNet time" were not configured to synchronize with the central time server.

We found that while USITC has implemented a time source for the network, not all systems are configured to synchronize with this central time source.

Recommendation 3:

Configure all ITCNet devices to synchronize with a central time source.

Management Comments and Our Analysis

On April 19th, 2011, Chairman Deanna Tanner Okun provided management comments to the draft audit report. The Chairman agreed that there are deficiencies in the Commission's Log Management Program that need to be corrected improve its effectiveness.

Based on the recommendations we made in our draft report, the Office of the CIO has resolved the issues with clock synchronization, and has added systems to the infrastructure being monitored.

Objective, Scope, and Methodology

Objective:

"Are system logs configured and monitored in a way that adds value to the operation of ITCNet?"

Scope:

This audit focused on the operational management of logs created on USITC systems as of February 7th, 2011 with a primary focus on the logging capabilities of critical infrastructure, including Active Directory Domain controllers, authentication devices, network infrastructure, security device infrastructure, and other devices critical to the core functions of USITC.

Methodology:

a. Interview program staff responsible for logging.
b. Interview operational staff receiving logs.
c. Collect inventory of network infrastructure devices.
d. Identify primary log management system in use.
e. Assess log management status of core infrastructure.
f. Identify and analyze logging on Active Directory authentication servers.
g. Review logging capabilities of RSA authentication servers.
h. Identify existing network time protocol server(s).
i. Assess time synchronization of infrastructure devices with the network time protocol server(s).
j. Review syslog settings of devices forwarding to primary log management system.

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

CO76-JJ-022

April 19, 2011

MEMORANDUM

TO: Philip M. Heneghan, Inspector General

FROM: Deanna Tanner Okun, Chairman

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

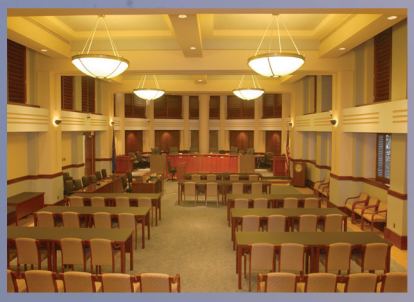
I am in receipt of the Inspector General's draft report, *Audit of Log Management*, dated March 25, 2011. I appreciate the opportunity to review the draft report and to provide comments.

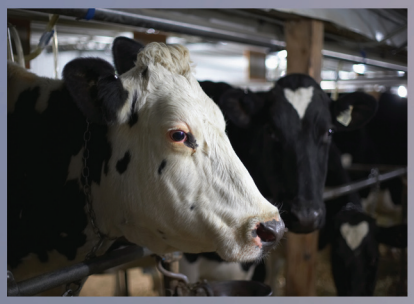
The Inspector General's draft report identified three problem areas related to the effectiveness of the Log Management. I concur with your assessment and appreciate that your office identified that 1) server, network, and security infrastructure is not being centrally monitored with the Commission's designated Log Management tool; 2) log data is not being effectively used; and 3) Clock synchronization is not fully implemented on ITCNet. It is an important goal of the Commission to have an effective Log Management Program. As you found, the agency has been proactively establishing and improving this program; however, several deficiencies remain that must be corrected.

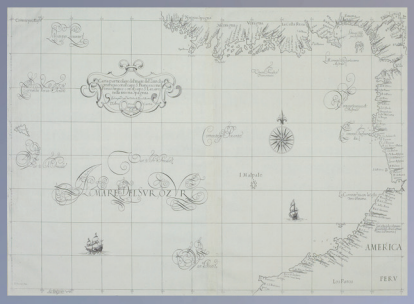
Thank you for reviewing the Log Management Program and making recommendations to strengthen its effectiveness.

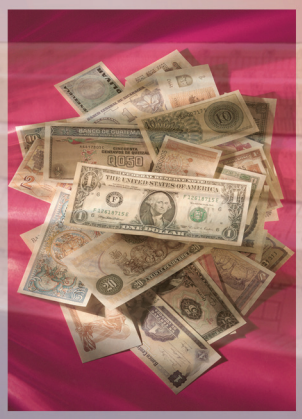
"Thacher's Calculating Instrument" developed by Edwin Thacher in the late 1870s. It is a cylindrical, rotating slide rule able to perform complex mathematical calculations involving roots and powers quickly. The instrument was used by architects, engineers, and actuaries as a measuring device.

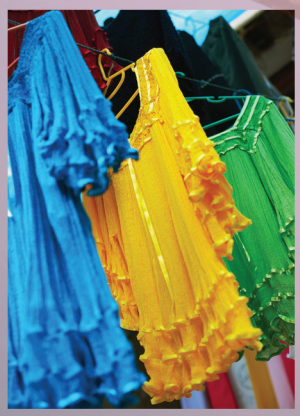
To Promote and Preserve the Efficiency, Effectiveness, and Integrity of the U.S. International Trade Commission











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

Office: 202-205-6542
Fax: 202-205-1859
Hotline: 877-358-8530
OIGHotline@USITC.gov