U.S. International Trade Commission

Audit of ITCNet's Security Log Management System

OIG-AR-21-08

April 19, 2021

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

April 19, 2021 IG-TT-006

Chair Kearns:

This memorandum transmits the final report for the Audit of ITCNet's Security Log Management System, OIG-AR-21-08. In finalizing this report, we analyzed management's comments to our draft report and have included those comments in their entirety as Appendix A.

The objective of the audit was to determine whether the Commission effectively collects, analyzes, and reviews its core infrastructure system security logs. The audit determined that the Commission had not effectively managed its core infrastructure system security logs.

The report contains 4 recommendations to improve managing core infrastructure system security logs. In the next 30 days, please provide me with your management decisions describing the specific actions that you will take to implement each recommenation.

Thank you for the courtesies extended to my staff during this review.

Michael J. Haberstroh
Acting Inspector General

Table of Contents

Background 1

Results of Audit 2

Problem Area: 1 Core Infrastructure Systems Security Logs Were Missing 3

Problem Area: 2 Processes to Analyze and Review Security Logs Were Not Effective .. 4

Management Comments and Our Analysis 5

Objective, Scope and Methodology 5

Other Report Information 6

Appendix A: Management Comments 7

Background

A log is a record of the events occurring within an organization's systems and networks. Logs are composed of entries that contain specific information related to these events, such as new user accounts, service failures, and network connections. Many logs are related to computer security and are generated by a variety of sources, including antivirus software, firewalls and intrusion detection and prevention systems, operating systems on servers, workstations, and networking equipment.

Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing audits and forensic analysis, supporting internal investigations, establishing baselines to assist in identifying operational trends and other long-term problems. Organizations may also store and analyze certain logs to comply with Federal legislation and regulations, including the Federal Information Security Management Act.

The Commission uses a Security Information and Event Management (SIEM) tool called Splunk for collecting, analyzing, and reviewing core infrastructure system security logs. Splunk can help correlate log events to detect and investigate threats, identify anomalies on the network, and provide near real-time alerts when a security event of interest is triggered. This tool is used by many federal agencies and is included in DHS's Continuous Monitoring and Diagnostics (CDM) program.

The core infrastructure consists of all the systems that are instrumental to carrying out the Commission's mission. This includes workstations, servers, and network devices that support the Commission's daily operations, as well as Microsoft Office 365, which provides the Commission with email, file storage, and collaboration tools. The systems that have been categorized by the Commission as major applications were not assessed individually in the performance of this audit.

Results of Audit

The objective of this audit was to answer the question:

- Does the Commission effectively collect, analyze, and review its core infrastructure system security logs?

No, the Commission does not effectively collect, analyze, and review its core infrastructure system security logs.

To effectively collect core infrastructure system security logs, the Commission should have a process and procedure to identify information systems that need to be collected, the types of security logs to be collected, and a way to verify that the logs are being collected. It is also important to have a process for how security logs are reviewed, as well as defined roles and responsibilities for reviewing and communicating actionable events.

During our audit, we interviewed staff, reviewed Commission policies and procedures, and analyzed data from both Splunk and the Commission's reporting dashboard for log management. The table below provides a summary of the results for each of the core infrastructure security logs we reviewed and identifies whether the Commission fully met, partially met, or did not meet the criteria for effective implementation.

Table 1: Summary of Results

	Windows Servers	Windows Workstations	Linux Servers	Network Devices	Microsoft O365
Identify Core Security Logs	●	●	●	●	●
Collect Core Security Logs	◑	●	◑	◑	●
Analyze and Review Logs	◑	◑	◑	◑	◑
Legend:	● Fully Met ◑ Partially Met ○ Not Met				

Based on these results, we found that the Commission did not effectively collect, analyze, or review the core infrastructure security logs. We identified two problem areas: (1) Core Infrastructure Systems Security Logs Were Missing; (2) Processes to Analyze Security Logs Were Not Effective. Each of these problem areas are discussed in detail in this report.

Problem Areas

Problem Area: 1

Core Infrastructure Systems Security Logs Were Missing

One of the keys to an effective log management program is to ensure the Commission is continually collecting logs from the core infrastructure security systems. To determine if the Commission was collecting all the core infrastructure security logs, we obtained the list of approved hardware devices authorized to run on ITCNet from the Office of the Chief Information Officer. We then compared that list to the core infrastructure system security logs being collected by Splunk.

We identified 18 out of 111 Windows servers that were on the approved hardware list that were not having their system security logs collected. We selected a judgmental sample of 25 Linux and network devices from the approved list and identified 15 devices that did not have any evidence of the system security logs being collected.

We found that the Commission did not have any controls in place to identify when core infrastructure security logs were not being collected. Failing to collect all core infrastructure security logs negatively impacts the Chief Information Officer's ability to identify or trace inappropriate or unauthorized activity on the servers. The Commission may be blind to disruptive event activity that could impact the confidentiality, integrity, and availability of the Commission's network. Additionally, it reduces the Commission's ability to perform incident response and forensic analysis to detect and analyze potential and active threats in a timely manner.

Recommendation 1: The Office of the Chief Information Officer implement a technical control to provide automated alerts to identify when core infrastructure system security logs are not being collected.

Problem Area: 2

Processes to Analyze and Review Security Logs Were Not Effective

The Office of the Chief Information Officer needs to have a process to analyze all the security logs collected; this process begins by creating "Use Cases". The term "Use Case" refers to an automated query that aggregates security log data to identify events of interest and abnormal activity on the network. Commission "Use Cases" are maintained in Splunk and are designed to provide an automatic alert when an event of interest is triggered.

The Office of the Chief Information Officer is responsible for the design and implementation of control activities related to log management. Based on our interviews with the security team, we learned the "Use Cases" were developed in an ad hoc manner at the discretion of the staff's judgment, rather than a solid methodology based on risk. As a result, they did not have documentation to identify the objective or business need of the "Use Case", the data sources related to the event, or a documented workflow of roles and responsibilities to guide the resolution of problems with other divisions within the Office of the Chief Information Officer when an event of interest was triggered.

For an event to be of interest it needs to be significant, timely, relevant, and correlated to potentially risky network activity that may require action. Our review of the 24 information security "Use Cases" in Splunk found:

- 13 did not have established baselines—information did not provide any context to analyze.
- 4 had not been updated to reflect changes to the environment—information was not relevant to current configuration.
- 2 did not provide useful or actionable information and as a result were not being reviewed or analyzed by the analyst—information was not actionable.
- 24 lacked an automatic alerting feature when a critical event was triggered—information did not allow for a timely response.

Based on this evidence, we determined the implementation of the Commission's "Use Cases" were not designed to provide actionable alerts from the aggregation of security log events.

Recommendation 2: Establish roles and responsibilities for security analysts and OCIO divisions for analyzing and reviewing events of interest.

Recommendation 3: Document the objective for each "Use Case" and the actions to be taken when events of interest are triggered.

Recommendation 4: Develop near real-time alerts for events of interest that are high risk to the Commission.

Management Comments and Our Analysis

On April 16, 2021, Chair Jason Kearns provided management comments on the draft report. He agreed with the findings in the audit that the Commission did not effectively collect, analyze, or review the core infrastructure security logs. He also stated that the Commission will make management decisions to address the four recommendations in the report.

Objective, Scope and Methodology

Objective:

Does the Commission effectively collect, analyze, and review its core infrastructure system security logs?

Scope:

The scope of this audit conducted from February 2020 through October 2020 was to assess the Commission's core infrastructure system security logs. These systems consisted of Windows workstation and servers, Linux servers, network devices, and Office 365 that are part of the Commission's core infrastructure.

Methodology:

To accomplish this objective, we:

- Reviewed security log process and procedures and interviewed the Chief Information Office staff to gain an understanding of the Commission's core infrastructure.
- Analyzed the core infrastructure authoritative hardware list and compared it to the systems in the Commission's Security Information Event Management (SIEM) system to determine if core security logs were being collected.
- Reviewed the security log documentation of what logs were to be collected and compared it to what logs were being captured by the Commission's SIEM.
- Analyzed the "Use Cases" in the Commission's SIEM to determine if they were effective and actionable.

Other Report Information

GAGAS Statement:

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.

Assessment of Internal Control:

We assessed internal controls as necessary to satisfy the audit objective. In particular, we assessed the design, implementation, and effectiveness of internal control component 3, control activities, principle 10, management should design control activities to achieve objectives and respond to risk. Any weaknesses or deficiencies noted are presented in the audit report. Since our review was limited to this specific internal control component and underlying principle, it may not have disclosed all internal control weaknesses that may have existed at the time of this audit.

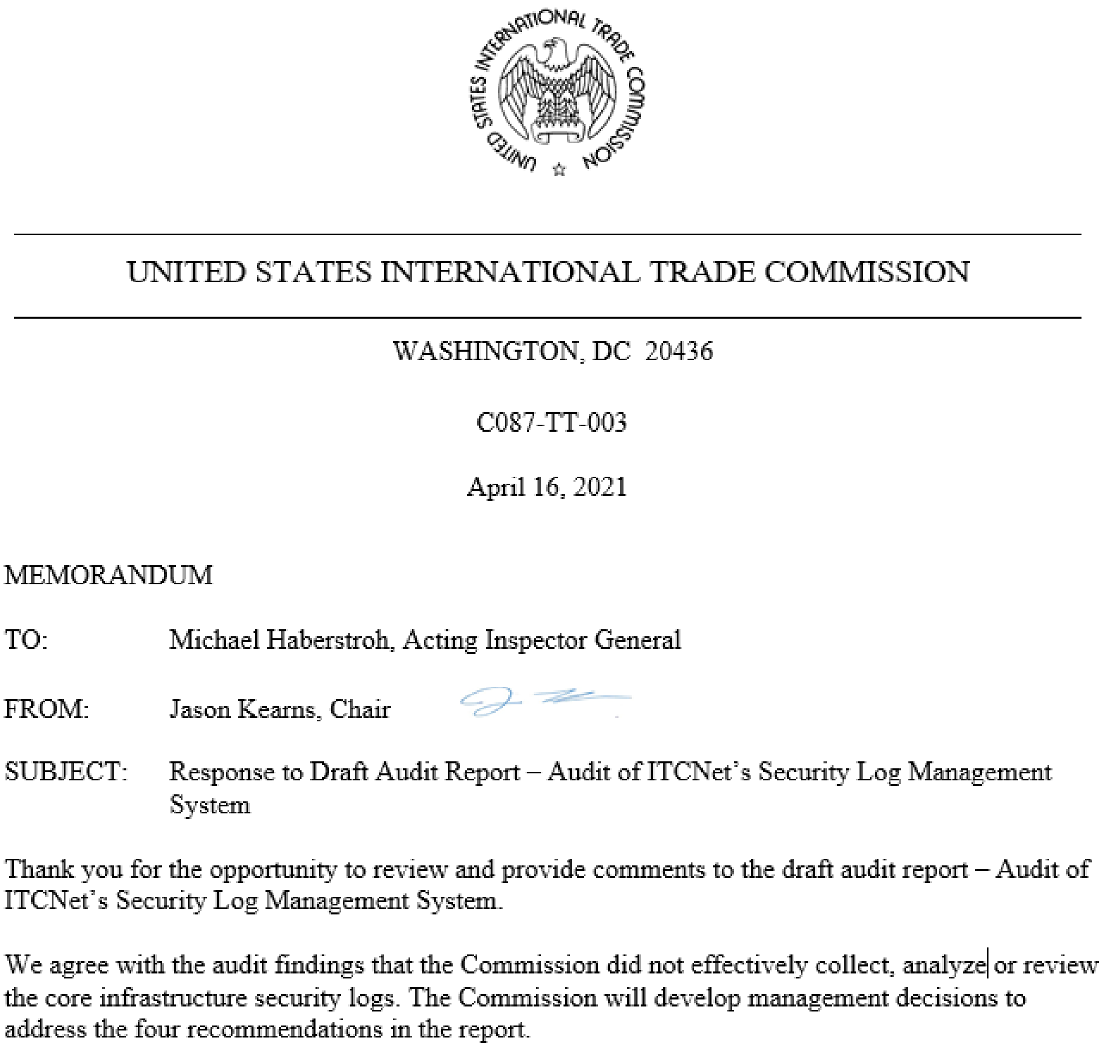
Reliability of Computer-Generated Data:

We assessed the reliability of Windows workstation and servers, Linux servers, network devices, and O365 core infrastructure system security logs by reviewing procedures and interviewing staff knowledgeable in this area. We determined that the data was reliable for this audit.

Sampling Methodology:

To determine if logs were being collected, we reviewed 100% of the information for Windows workstations and Windows servers. We performed a judgmental sample of Linux servers and network devices, as such any findings related to the Linux servers and network devices cannot be projected to the population.

Appendix A: Management Comments



UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

C087-TT-003

April 16, 2021

MEMORANDUM

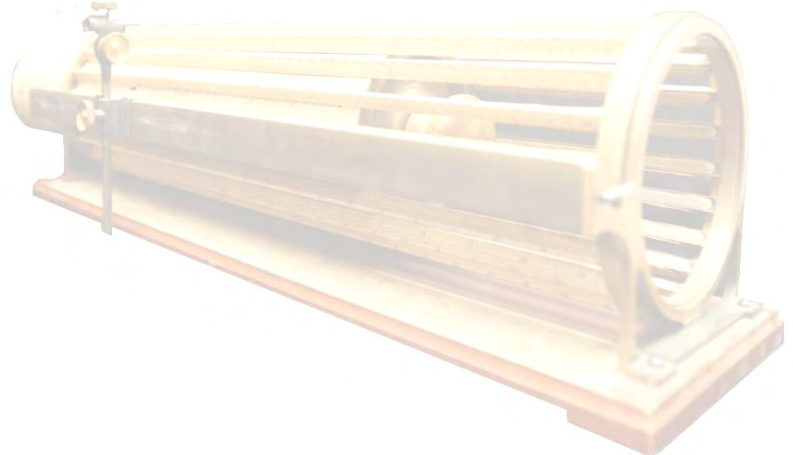
TO: Michael Haberstroh, Acting Inspector General

FROM: Jason Kearns, Chair

SUBJECT: Response to Draft Audit Report – Audit of ITCNet's Security Log Management System

Thank you for the opportunity to review and provide comments to the draft audit report – Audit of ITCNet's Security Log Management System.

We agree with the audit findings that the Commission did not effectively collect, analyze or review the core infrastructure security logs. The Commission will develop management decisions to address the four recommendations in the report.



"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: 202-205-2210
Fax: 202-205-1859
Hotline: 202-205-6542
OIGHotline@USITCOIG.GOV