U.S. International Trade Commission

Evaluation of Public Website Security

OIG-ER-16-13

July 25, 2016

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

Irving A.Williamson, Chairman
Dean A. Pinkert
David S. Johanson
Meredith M. Broadbent
F. Scott Kieff
Rhonda K. Schmidtlein

UNITED STATES INTERNATIONAL TRADE COMMISSION

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20436

July 25, 2016 IG-OO-022

Chairman Williamson:

This memorandum transmits the final report for the Evaluation of Public Website Security, OIG-ER-16-13. 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 evaluation was to determine whether the Commission had effectively secured its public websites. The evaluation determined that the Commission had effectively secured these websites, and identified two areas for improvement.

This report contains three recommendations to further improve its public website security. 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 evaluators during this review.

Philip Heneghan

Philip M. Heneghan
Inspector General

Table of Contents

Results of Evaluation

The purpose of this audit was to answer the question:

- Does the Commission effectively secure its public websites?

Yes, the Commission effectively secures its public websites.

To effectively secure its network, including its public websites, the Commission must implement a number of controls. These include the top four controls rated as “very high” for the mitigation of attacks by the National Security Agency (NSA), which compose the following:

1. Inventory of Authorized and Unauthorized Devices:
    - Know the devices on your network.
2. Inventory of Authorized and Unauthorized Software:
    - Know the software on your network.
3. Secure Configurations for Hardware & Software on Laptops, Workstations, and Servers:
    - Secure systems by default.
4. Continuous Vulnerability Assessment and Remediation:
    - Monitor and patch continuously.

To securely manage its public websites, the Commission must:

1. Know which sites it publishes.
2. Know the software and hardware infrastructure providing these web services.
3. Securely configure the hardware and software infrastructure providing web services.
4. Continuously diagnose and mitigate vulnerabilities affecting its web services.

The Commission:

1. Provided a complete inventory of its web applications.
2. Provided a complete inventory of the servers providing web services.
3. Achieved low vulnerability scores for its infrastructure.
4. With only two exceptions out of 43 servers, performed continuous mitigation and diagnostics of its network.

The Commission’s inventory of public websites encompassed all websites discovered by our search for Commission website applications. The Commission’s System Engineering Division centrally managed all website applications and maintained an accurate inventory of its 13 websites and 43 servers providing these services.

The Commission hosts several highly sensitive websites that are critical to its mission and possess confidential business data. Our assessment of these mission-critical websites identified no high severity vulnerabilities, giving further evidence that the System Engineering Division effectively wrote secure code and resolved findings from previous external scans.

While our scans detected minor vulnerabilities in the web applications, the nature of these detected vulnerabilities would not result in the exploitation of the Commission's infrastructure.

With only two exceptions out of 43 servers, the Commission performed continuous diagnostics and mitigation of vulnerabilities. Of the 41 servers measured, the scans identified 40 high-severity vulnerabilities, or just slightly less than one per host. This is well below the Commission's stated target of two or less high-severity vulnerabilities per host.

While the Commission has effectively secured its public websites, we did identify two areas for improvement, which include: (1) perform credentialed scans for all hosts, and (2) perform internal web application security scanning.

Areas for Improvement

Area for Improvement 1:

Perform credentialed scans for all hosts.

Managing the security of a network requires continuous vulnerability scanning of all hosts on its network. Credentialed scanning provides an in-depth assessment of vulnerabilities related to installed software on a host. While the Commission performs credentialed scans on nearly all infrastructure, we found that two hosts had failed these credentialed scans.

Failure of credentialed scans can result in what appears to be a "clean" scan, i.e., no vulnerabilities were discovered and reported. The failure of a credentialed scan can lead to an incorrect belief that the host possesses no known vulnerabilities, when in fact, the host could have multiple vulnerabilities, but this knowledge is unavailable to the Commission. This lack of vulnerability information results in a higher level of uncertainty and risk to the Commission.

The Commission's continuous scanning tools have the ability to report on hosts failing credentialed scans. Using the *Credentialed Scan Failures* report generated by this tool, we identified the two hosts failing credentialed scans. After discussions with CIO staff, we found that these hosts had not received credentialed scans for a period of approximately six weeks.

Recommendation 1: The Chief Information Security Officer report the presence of failed credentialed scans to appropriate management in a timely fashion.

Recommendation 2: The Network Services Division resolve failed credentialed scans in a timely fashion.

Area for Improvement 2:

Perform internal web application security scanning.

The Commission currently relies on external providers to perform web application vulnerability assessments. The results from this type of testing can provide prioritized areas for inspection and remediation to maintain and strengthen the security of custom-coded web application software. The Commission’s external web security assessments were of two varieties: one in-depth scan as part of a one-time (or infrequent) assessment, and weekly scans using a tool with limited web application security testing functionality.

To improve security, public websites should be assessed on a continual basis using tools and methodology specific to web application security testing. An organization performing software development should also perform continuous code testing during software development to ensure that the code is written securely throughout the software development life cycle. While the Commission has leveraged external providers to perform limited tests against its public websites, it has not been performing incremental and thorough testing of pre-deployed code.

Software tools used for website application testing can range from expensive, proprietary software to free, open-source tools. Cost-effective application security testing tools exist that can perform customized in-depth testing of code as it is being developed, enabling efficient development and continuous monitoring of the Commission’s custom code. The Commission possesses the skill sets needed to perform this testing. If the Commission were to employ its own continuous testing, it could more quickly become informed of vulnerabilities in its custom code, enabling it to identify vulnerabilities rapidly and lower the ongoing level of risk to the Commission.

Recommendation 3: The Systems Engineering Division implement internal, focused security testing of web applications.

Management Comments and Our Analysis

On July 18, 2016, Chairman Irving Williamson provided management comments on the draft report. He agreed that the Commission could further improve upon its effective public website security by performing credentialed scans for all hosts and internal web application security scanning. He also agreed to make management decisions in response to the recommendations in the report.

Objective, Scope and Methodology

Objective:

Does the Commission effectively secure its public websites?

Scope:

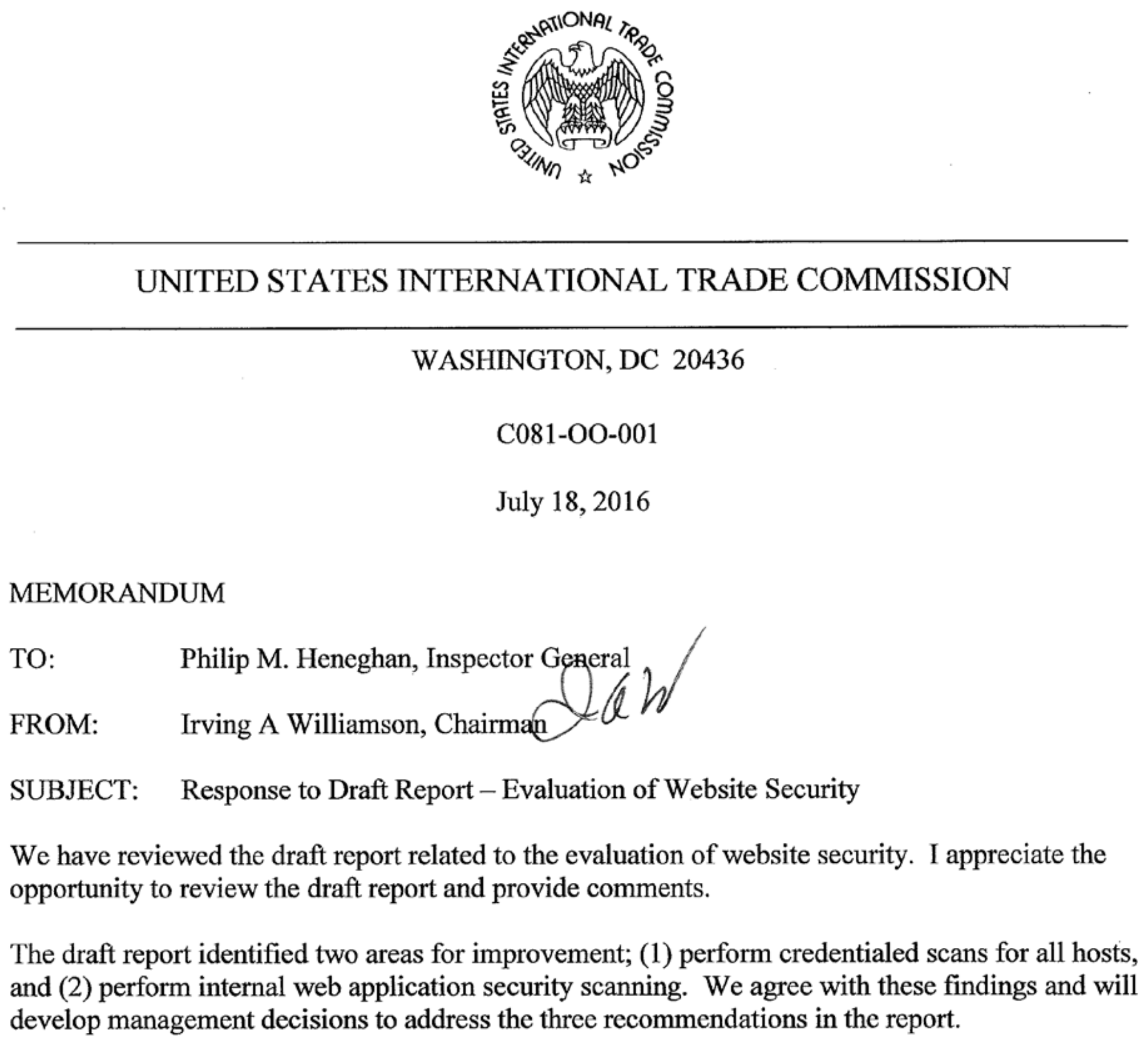
This audit assessed the management of all physical and virtual hardware connected to the public ITC network that had the ability to listen or transmit on the network.

Methodology:

1. Collected and analyzed Commission/CIO data:
   - Interviewed staff to determine public website infrastructure and security practices;
   - Collected inventory of server infrastructure supporting these websites;
   - Gathered existing vulnerability data;
   - Reviewed external scan data;
   - Performed analysis of collected data and reports.
2. Performed web application security testing with commercial and open source software tools.

This evaluation was performed as part of a concurrent government-wide review of agency website security sponsored by the Council of the Inspectors General on Integrity and Efficiency.

Appendix A: Management Comments on Draft Report



UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

C081-OO-001

July 18, 2016

MEMORANDUM

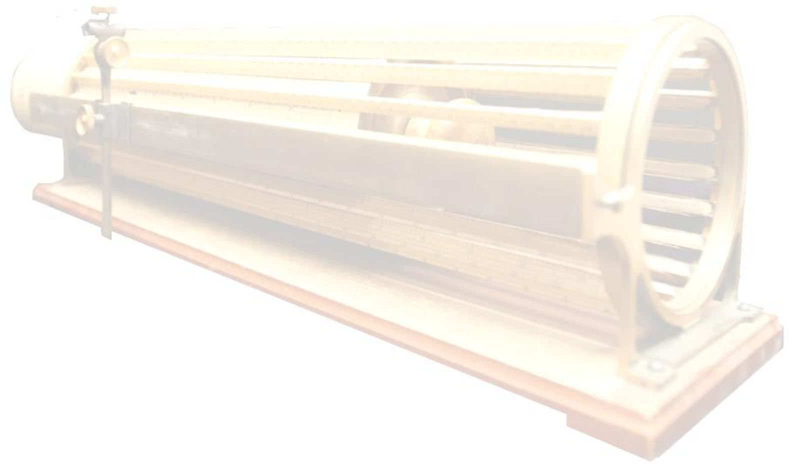
TO: Philip M. Heneghan, Inspector General

FROM: Irving A Williamson, Chairman

SUBJECT: Response to Draft Report – Evaluation of Website Security

We have reviewed the draft report related to the evaluation of website security. I appreciate the opportunity to review the draft report and provide comments.

The draft report identified two areas for improvement; (1) perform credentialed scans for all hosts, and (2) perform internal web application security scanning. We agree with these findings and will develop management decisions to address the three 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: 202-205-6542
Fax: 202-205-1859
Hotline: 202-205-6542
OIGHotline@USITC.GOV