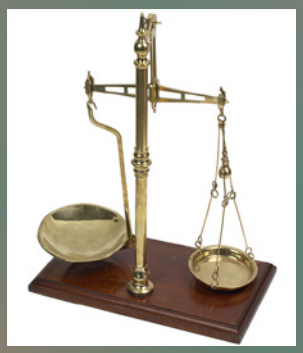
U.S. International Trade Commission

Assessment of USITC Website Encryption



OIG-MR-16-10 **February 10, 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.

UNITED STATES INTERNATIONAL TRADE COMMISSION

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20436

February 10, 2016 IG-OO-004

Chairman Broadbent:

Attached for your information is the final report, Assessment of USITC Website Encryption, OIG-MR-16-10. This assessment focused on whether the Commission effectively encrypted its websites.

In finalizing this report, we analyzed management's comments to our draft report and have included those comments in their entirety as Appendix A. This assessment determined that the Commission did not effectively encrypt its secure websites. We are issuing this report to inform you of the results of our assessment.

This report contains two 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 office during this review.

Philip M. Heneghan
Inspector General

Table of Contents

Background

On June 8, 2015, OMB issued Memorandum M-15-13, titled "Policy to Require Secure Connections across Federal Websites and Web Services." This memo requires all federal agencies to enforce encrypted access to their websites by December 31, 2016 using HTTP Strict Transport Security (HSTS).

As part of the government-wide effort to protect the privacy and integrity of public web connections, OMB established a public dashboard to monitor agency compliance at https://pulse.cio.gov. This dashboard provides status of agency efforts to encrypt public websites and a letter grade assessment of that encryption by a public assessment site, SSL Labs.

The OMB assessment of the usitc.gov website as of January 15, 2016 was as follows:

Domain	Uses HTTPS	Enforces HTTPS	Strict Transport Security (HSTS)	SSL Labs Grade
usitc.gov	Yes	Yes	No	F

The OMB assessment determined that the website usitc.gov enforces secure traffic, but does not require HTTPS Strict Transport Security and fails a comprehensive third-party assessment.

As new technologies and decryption methods proliferate, what was once seen as secure becomes known to be vulnerable, and newer encryption methods are introduced to overcome identified flaws. Website encryption strategies are complex, so expertise is required to implement and maintain strong encryption methods for a website. Because the effectiveness of a specific method of encryption can degrade over time, it is important to periodically reassess whether encryption methods in use continue to be effective.

The OMB requirement is to secure traffic to Federal websites. This traffic can only be secure if effective encryption is deployed.

Results of Review

The objective of this assessment was the answer the question:

- Does the Commission effectively encrypt its public websites?

No, the Commission did not effectively encrypt any of its 10 public websites.

On January 20, 2016 we identified 10 public websites encrypted by the Commission, and tested each of these encrypted websites to determine the effectiveness of that encryption.

Using free, publicly available tools such as Nmap 7.0 and the website SSLLabs.com, we identified a range of problems, some serious, with all of the Commission's encrypted websites. These issues included minor problems such as incomplete server certificate chains, significant issues such as allowing SSL 3 (Secure Sockets Layer version 3), and severe problems such as pervasive vulnerability to POODLE TLS attacks (Padding Oracle On Downgraded Legacy Encryption). For the purpose of this report, we evaluated the effectiveness of encryption based on the OMB-referenced SSL Labs Grade. An 'A' grade would indicate effective encryption.

The effectiveness of encryption for each Commission website is as follows:

Website	Effectiveness of Encryption	Notes:
https://dataweb.usitc.gov	Ineffective	
https://dropbox.usitc.gov	Ineffective	
https://edis.usitc.gov	Ineffective	
https://hts.usitc.gov	Ineffective	
https://itcmail2.usitc.gov	Ineffective	
https://parkinglot.usitc.gov	Ineffective	
https://remote.usitc.gov	Ineffective	
https://srmm.usitc.gov	Ineffective	Website resulted in endless redirects.
https://surveys.usitc.gov	Ineffective	
https://www.usitc.gov	Ineffective	

We confirmed the results generated by SSLLabs.com by running specific tests using Nmap.

To secure its public websites and achieve the goals of the OMB mandate, the Commission should ensure it implements effective encryption, and remove those methods of encryption that do not meet the standard.

Recommendation 1: The CIO deploy only effective encryption to all Commission websites.

Recommendation 2: The CIO establish a process to perform routine testing of Commission website encryption.

Management Comments and Our Analysis

On February 8, 2016, Chairman Meredith Broadbent provided management comments on the draft report. She acknowledged that the Commission did not have effectively encrypt its secure websites and agreed to make management decisions to address the recommendations in the report.

Objective, Scope, and Methodology

Objective:

- Determine whether Commission public website encryption was effective.

Scope:

- Websites available from the public Internet hosted in USITC network range.

Methodology:

1. Identified Commission's public websites using encryption.
2. Performed assessment using SSLLabs.com
3. Performed assessment using Nmap 7.0.
4. Verified and correlated results.

Appendix A: Management Comments on Draft Report

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

C084-OO-002

February 8, 2016

MEMORANDUM

TO: Philip M. Heneghan, Inspector General

FROM: Meredith M. Broadbent, Chairman

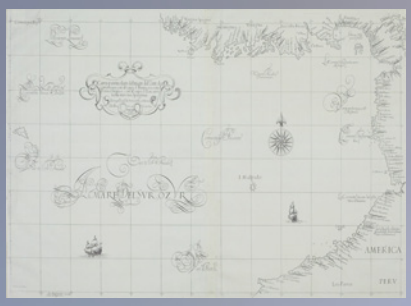
SUBJECT: Response to Draft Management Letter Report – Assessment of USITC Website Encryption

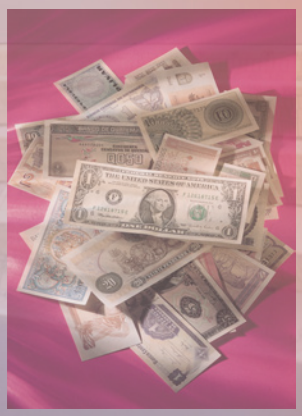
We have reviewed the management letter of the assessment of USITC's secure websites. I appreciate the opportunity to review the report and provide comments.

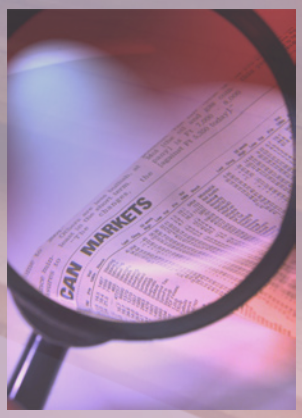
We agree that the Commission did not effectively encrypt its secure websites. The Commission will implement effective encryption on its websites and remove weak methods of encryption. We understand that OMB has issued a standard for Federal website encryption and we will develop management decisions using that standard to address the recommendations in the report.

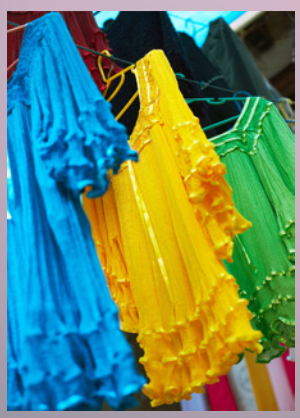
"Thacher's Calculating Instrument" developed by Edwin Thacher in the late 1870s. It is a cylindrical, rotating slide rule able to quickly perform complex mathematical calculations involving roots and powers quickly. The instrument was used by architects, engineers, and actuaries as a measuring device.

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