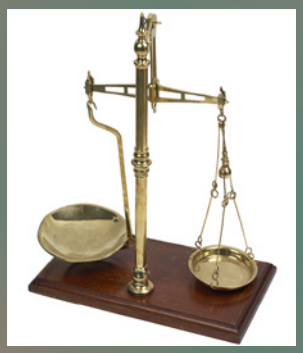
U.S. International Trade Commission

Report to Congress for Cybersecurity Act of 2015



OIG-MR-16-14

August 12, 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
David S. Johanson, Vice Chairman
Dean A. Pinkert
Meredith M. Broadbent
F. Scott Kieff
Rhonda K. Schmidtlein

OFFICE OF INSPECTOR GENERAL

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

Via Electronic Transmission

August 12, 2016

IG-OO-024
OIG-MR-16-14

Dear Chairman Williamson:

We are issuing this management report to provide you the same information we provided to Congress as required by the Cybersecurity Act of 2015.

The Cybersecurity Act of 2015, requires the Inspectors General of agencies with a computer system that provides access to personally identifiable information to submit each year a report on the topics related to the measures employed by agencies to protect this data to the appropriate committees of jurisdiction in the Senate and the House of Representatives.

We have included our Report to *Congress for Cybersecurity Act of 2015* as an attachment .

Philip M. Heneghan
Inspector General
U.S. International Trade Commission

OFFICE OF INSPECTOR GENERAL

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

Report to Congress for Cybersecurity Act of 2015

This report is required by the Cybersecurity Act of 2015, which directs the Inspectors General of agencies with a computer system that provides access to personally identifiable information are to submit each year a report on the topics related to the measures employed by agencies to protect this data to the appropriate committees of jurisdiction in the Senate and the House of Representatives.

This report is focused on the U.S. International Trade Commission's (USITC) General Support System (GSS) which is an unclassified network that processes personally identifiable information (PII).

Our responses to the questions from the Cybersecurity Act of 2015 are as follows:

(A) A description of the logical access policies and practices used by the covered agency to access a covered system, including whether appropriate standards were followed.

a. The USITC policies on logical access include:
    i. Permanent staff are issued HSPD-12 identification cards, which are required for (1) physical access to the building and offices, and (2) are for logical access to the USITC network using USITC workstations.
    ii. Temporary staff are not issued HSPD-12 identification cards, and are required only to possess a username and password for logical access to the USITC network. These staff are required to present identification to access the physical facility where USITC workstations are present.
    iii. Remote desktop and application access to the USITC network requires multi-factor authentication for all staff, both permanent and temporary.
    iv. Remote access to email via smartphones and other devices does not use multi-factor authentication, requiring only username and password.
    v. The USITC practices generally follow the policies.
b. Appropriate standards were followed.

(B) A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.

a. The USITC policy regarding logical access to systems by privileged users:
   i. Privileged users require an HSPD-12 identification card, with a distinct username and password for on-site logical system access.
   ii. Remote desktop and application access to the USITC network requires multi-factor authentication for all staff, both permanent and temporary. Once logged in, privileged account use requires only a username and password.

(C) If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.

a. N/A

(D) A description of the following information security management practices used by the covered agency regarding covered systems:

(i) The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.

(I) The USITC policy is to use automated applications to gather the authorized software inventory. As part of the authorization process, their policy is to compare stored licensing information to a count of software installation instances detected on the network. An audit we issued on August 11, 2015 concluded that the Commission did not use software inventory to manage its network. The Commission made management decisions for recommendations in our report, and they have reported the completion of final action on the majority of those decisions. *https://www.usitc.gov/sites/default/files/oig/documents/oig-ar-15-12.pdf*

(ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including—

(I) data loss prevention capabilities;

i. In testing, we found that USITC does not have the capability to detect or prevent even the most basic means of the exfiltration of PII.

(II) forensics and visibility capabilities; or

i. The USITC has limited forensics capabilities. It does possess some tools that record and analyze network traffic, depending on the nature of the traffic. It does not store a record of all network traffic and system events.

(III) digital rights management capabilities.

i. The USITC does not have any digital rights management capabilities, and stated that they do not require this type of protection.

(iii) A description of how the covered agency is using the capabilities described in clause (ii).

(I) The USITC uses its limited forensics abilities primarily to try to understand the nature of access performed against its web servers when atypical network traffic is detected, and in limited circumstances to understand recent logged events on its servers and workstations.

(iv) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.

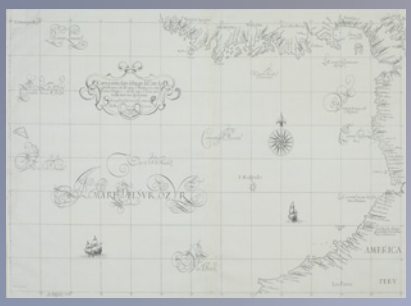
(I) The majority of USITC work does not involve the processing of classified materials or PII. The USITC has been focused on the fundamentals of securing its network, including authorized software/hardware inventories, application whitelisting, secure configurations, and continuous diagnostics and mitigation.

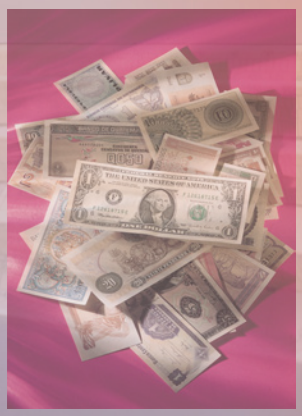
(E) A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph (D).

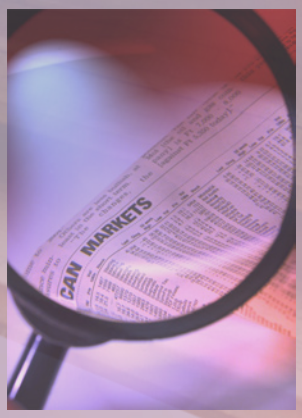
a. The USITC states that contracts issued by USITC that involve access to PII or sensitive data include standard language stating all contractors are required to adhere to "all applicable Federal laws or agency rules, processes and procedures" as regards information security, and all contractors with ITCNET access are required to comply with the (general logical access) controls.

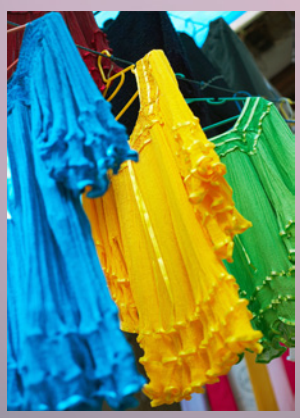
"Thacher's Calculating Instrument" developed by Edwin Thacher in the late 1870s. It is a cylindrical, rotating slide rule able to quickly perform complex mathematical calculations involving roots and powers quickly. The instrument was used by architects, engineers, and actuaries as a measuring device.

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