U.S. International Trade Commission

Audit of Continuous Monitoring

OIG-AR-11-15

September 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.

Commissioners

Deanna Tanner Okun, Chairman
Irving A. Williamson, Vice Chairman
Charlotte R. Lane
Daniel R. Pearson
Shara L. Aranoff
Dean A. Pinkert

UNITED STATES INTERNATIONAL TRADE COMMISSION

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20436

VIA ELECTRONIC TRANSMISSION

September 28, 2011 OIG-JJ-017

Chairman Okun:

This memorandum transmits the Office of Inspector General's final report Audit of Continuous Monitoring, OIG-AR-11-15. 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 four 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 **1**

Problem Areas **2**

Problem Area 1: The Commission does not produce a real-time executive dashboard. 2

Problem Area 2: The Commission does not provide automated data feeds to CyberScope. 2

Management Comments and Our Analysis **3**

Scope and Methodology **4**

Appendix A: Management Comments on Draft Report ..... **A**

Results of Audit

Has the USITC implemented an effective and comprehensive continuous monitoring system?

No. The USITC has not implemented an effective and comprehensive continuous monitoring system.

Continuous monitoring describes the process of constantly collecting and auditing raw data. In a typical computer network, systems generate logs to record a range of events, including network access attempts, changes in permissions, or the starting and stopping of programs. The sheer volume of events dictates a need for specialized software to collect, store, and analyze this data. While specialized technicians have the training and skillsets to review this raw data, it can be indecipherable to management not involved in the day-to-day operations of complex networks. If management does not have real time access to what is happening on its systems--it is not managing those systems.

For this reason, the Office of Management and Budget (OMB) recently instituted a requirement for Federal Agencies to perform continuous monitoring, to provide specific summary data in the form of an executive dashboard, and to provide direct feeds of this data to OMB's CyberScope portal. CyberScope is a web portal designed to collect government-wide information security data.

To effectively implement OMB's continuous monitoring requirements, the Commission must perform the following:

1. Automated log management of all core infrastructure.
2. Automated management of software inventory.
3. Management of hardware inventory.
4. Inventory external connections.
5. Collect and maintain data concerning security training.
6. Collect and maintain data concerning identity management and access.
7. Create a real-time executive dashboard.
8. Configure capable software to provide data feeds to CyberScope.

We identified two problem areas that must be resolved before the Commission can meet continuous monitoring requirements: it does not currently produce a real-time executive dashboard, and it does not yet have the capacity to provide data feeds to the CyberScope portal.

Problem Areas

Problem Area 1:

The Commission does not produce a real-time executive dashboard.

The Office of Management and Budget requires agencies to implement an executive dashboard that presents management with summary data in a manner that enables timely decision making. This data should be presented in a form that is automatically updated, provides historical data for context, and highlights areas critical to decision making.

The Commission does not currently have this capability. A prototype dashboard has been produced using a Microsoft Excel spreadsheet, but this format does not have the capability to display real-time data, and does not provide an easily viewed historical context to enable educated decision-making. Development of an effective executive dashboard has not been a priority for the Office of Enterprise Security Management, and the end result is a product that is not being used by the CIO.

Recommendation 1:

Present the data in a real-time format, such as an automatically updating webpage.

Recommendation 2:

Provide data on the dashboard using time-based graphs to allow those viewing it to identify trends and gain perspective.

Problem Area 2:

The Commission does not provide automated data feeds to CyberScope.

OMB requires agencies to provide data feeds to CyberScope for specific data including inventory, systems and services, hardware, software, external connections, security training, and identity management and access.

This requires that agencies implement management software to collect this data. The USITC is collecting the majority of data required by OMB, but it does not yet have the capacity to provide OMB with automated data feeds. The Commission will need to configure its software to push its data to CyberScope automatically where possible, and will need to provide manual data feeds for data items that cannot be automated.

Recommendation 3:

Configure management software to push data to CyberScope.

Recommendation 4:

Prepare manual data feeds for data items that cannot be automated.

Management Comments and Our Analysis

On September 27, 2011, Chairman Deanna Tanner Okun provided management comments on the draft audit report. The Chairman agreed with our assessment that there are two problem areas related to the lack of an executive dashboard or data feeds to Cyberscope, and recognized that the Commission can implement effective continuous monitoring by implementing the recommendations detailed in the two problem areas. The Chairman's response is provided in its entirety as Appendix A.

Scope and Methodology

Scope:

- The scope of this audit included the systems and processes related to Continuous Monitoring at the USITC.

Methodology:

a. Identify Continuous Monitoring and reporting systems in use at the USITC
b. Assess existing systems compliance with Office of Management and Budget Memorandum M-10-15 and NIST Special Publication 800-137, with a specific focus on the following areas:
    i. Executive dashboard
    ii. OMB FISMA reporting requirements
    iii. System-wide Continuous Monitoring/Automation
    iv. Measures and Metrics
    v. Finding analysis and response

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-048

September 27, 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 Continuous Monitoring"

I appreciate the opportunity to review the Inspector General's draft report, *Audit of Continuous Monitoring*, dated August 24, 2011, and to provide comments.

The Inspector General's draft report found that the Commission has not implemented a comprehensive, IT Security continuous monitoring program consistent with recently released guidance from the Office of Management and Budget (OMB). The report identified two areas for improvement: (1) the Commission does not currently produce a real-time executive dashboard, and, (2) it does not yet have the capacity to provide data feeds to the CyberScope portal.

We agree with the findings. The Commission is dedicated to ensuring that it builds a robust IT security program that both complies with OMB guidance and provide actionable information. Thank you for reviewing the Commission's implementation of OMB's continuous monitoring program and making the recommendations to strengthen its IT security activities.

"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