U.S. International Trade Commission

Audit of EDIS Security

OIG-AR-11-07

December 29, 2010

Office of Inspector General

OFFICE OF INSPECTOR GENERAL

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

VIA ELECTRONIC TRANSMISSION

December 29, 2010 OIG-HH-034

Chairman Okun:

This memorandum transmits the Office of Inspector General's final report Audit of EDIS Security OIG-AR-11-07. 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 eight 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 Heneghan

Philip M. Heneghan
Inspector General

Table of Contents

Results of Audit

The objective of this audit was to answer the question:

Is the EDIS web application properly secured?

EDIS is not properly secured. The security of a system is only as good as its weakest link. In the case of EDIS, a few specialized workstations with significant vulnerabilities have direct access to the EDIS infrastructure, placing the entire system at risk, and one workstation has autologon enabled for an administrator account.

The Commission has recently implemented a comprehensive process to measure and patch user workstations on ITCNet. In contrast, the specialized EDIS workstations incorporate software applications that cannot be maintained by Commission staff, but instead require maintenance by an outside vendor, during non-production hours. These conditions increase the level of effort required to schedule and perform vendor maintenance, leading to a situation where these systems have become the Achilles heel to the otherwise strong security of EDIS servers and supporting network infrastructure. Out of 40 nodes scanned on the EDIS network, only the five specialized workstations exhibited a high number of vulnerabilities.

The problem areas negatively affecting EDIS security include the lack of a comprehensive process to patch workstations, installations of obsolete software, task specific workstations not locked down, and automatic logon of an administrator account.

Problem Areas & Recommendations

Problem Area 1:
There is no comprehensive process for patching workstations.

Our review of the user-facing, specialized EDIS workstations found that all Windows XP systems were missing significant numbers of security patches. Five systems had a total of 137 High Severity Vulnerabilities. The vulnerabilities result primarily from missing patches for third-party applications, including Adobe Acrobat (and Reader), Adobe Flash, and Sun Java.

One system had 15 High Severity vulnerabilities related to missing patches for Microsoft software, dating back to April, 2009.

Recommendation 1:

Deploy a tool to continuously measure the patch status of all EDIS systems.

Recommendation 2:

Report monthly on patch status of all EDIS systems to all senior management officials in the Commission.

Recommendation 3:

Implement an effective patching process for all EDIS systems.

Problem Area 2:
There are obsolete software applications installed.

We found two software applications installed that are essentially or functionally obsolete. This includes Adobe Acrobat 7.1, which is no longer supported by Adobe, and Internet Explorer version 6.0, which has been replaced by version 8.0.

Adobe Acrobat 7.1 no longer receives vendor support, so vulnerabilities in this software will remain unpatched andexpose systems using this software to perpetual risk. This software should be updated and maintained to reduce its potential to serve as an attack vector.

Internet Explorer version 8.0 is Microsoft's current browser, and contains security technologies such as Data Execution Prevention designed to mitigate Internet threats. Internet Explorer 6.0 does not contain this technology, making it much more susceptible to known attacks. Systems using Internet Explorer 6.0 should be upgraded to use a modern, secure browser.

Recommendation 4:

Update or remove obsolete software.

Problem Area 3:
Task specific workstations are not locked down.

Specialized workstations are provided to staff for the bulk scanning of documents into the EDIS data repository, and for the creation of CD media to convey official EDIS records. Given their specific roles, these systems should not require access to the Internet (and the risks inherent in this access) to perform these functions. These systems should be restricted from Internet access.

Specific communication is required between these workstations and the back-end EDIS server network to store and retrieve EDIS data; however, the necessary communications do not require full, unrestricted access to the EDIS network. A best practice in security is to implement least-privilege access, which in this case would direct a very limited scope of communication ports. Least-privilege access is…… In order to enforce least-privilege, these workstations should be moved to an isolated network with firewall rules to allow only for specific, required access to key EDIS infrastructure.

Recommendation 5:

Deny Internet access to specialized systems that do not require this access to perform specific, work-related functions.

Recommendation 6:

Segregate user-facing systems to a network without direct, unrestricted access to critical back-end servers.

Problem Area 4:
One workstation has a feature enabling automatic logon of an administrative account.

Automatic logon was enabled on one workstation. This feature enables a computer to be turned on and logged in without entering a username and password. While this feature saves time and effort for users, it allows anonymous use of the system to anyone with physical access. In this instance, the account logged in is a local administrator, with full control of all aspects of the server. The combination of anonymous access, administrative privileges, and direct network access to the EDIS network make this workstation a serious and dangerous threat to the security of EDIS.

Recommendation 7:

Disable automatic logon.

Recommendation 8:

Remove administrative permissions for standard user accounts.

Scope and Methodology

Scope:

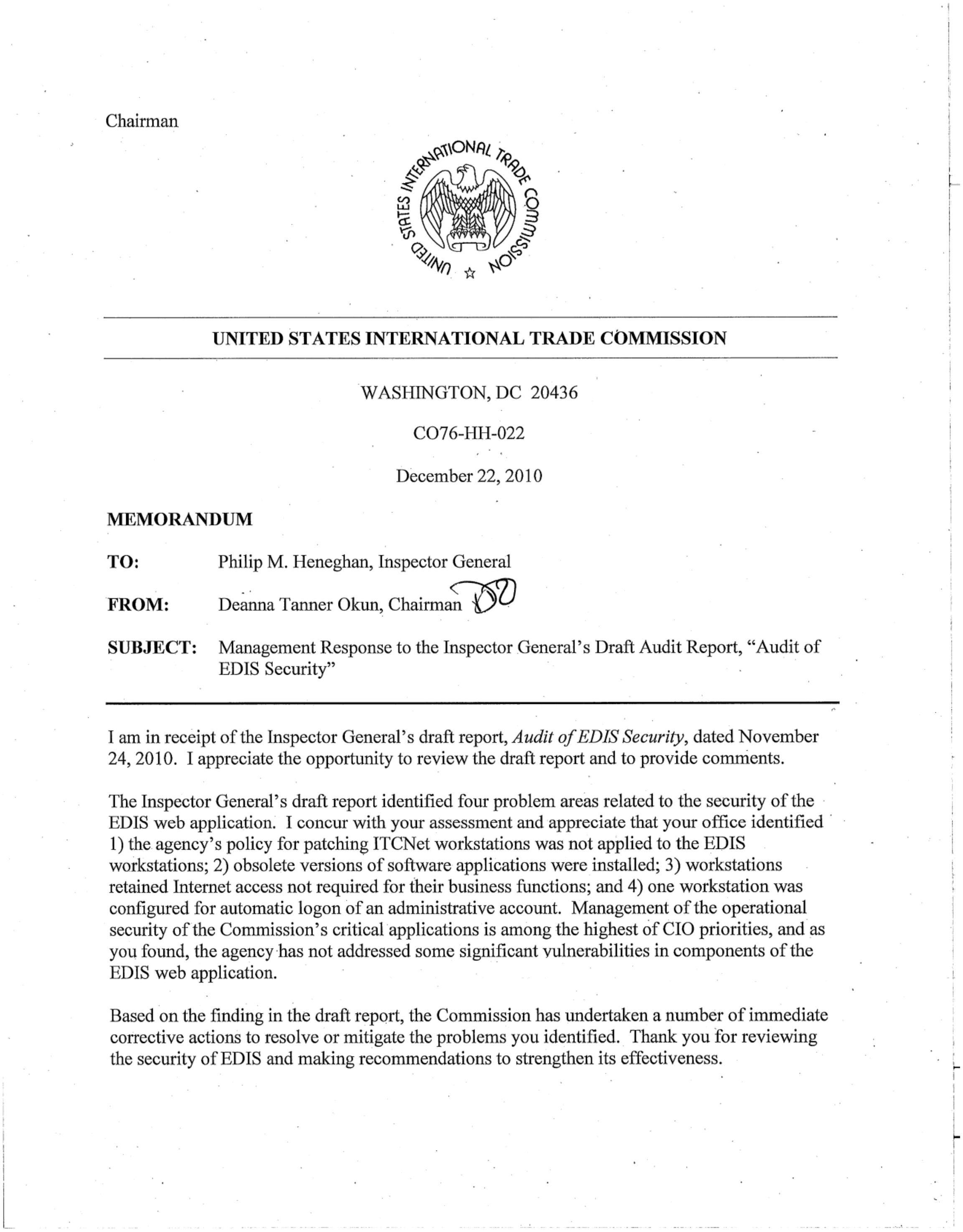
This audit focused on the EDIS application, and included the related systems and subsystems supporting the security of this application.

Methodology:

- We interviewed E-Business Division program staff, and worked with them to identify the structure of the network environment composing EDIS, the general history of the application, and to negotiate a methodology and timeline for targeted scanning of the application.
- We interviewed staff from the Network Support and Planning Division to identify target network ranges associated with the EDIS application and its supporting infrastructure.
- We interviewed staff from Dockets, who are responsible for the daily operations of the EDIS system.
- We interviewed end users of EDIS, including staff from the Offices of Investigations, General Counsel, and Unfair Import Investigations, asking them specifically about their experience using EDIS, and whether they had knowledge of security problems affecting the application.
- Between September 20th and 24th, 2010, we performed unauthenticated network and device discovery of the EDIS network using Nmap 5.35.
- From September 25th to October 4th, 2010, we performed authenticated vulnerability assessments of all EDIS network nodes using Nessus 4.2.
- We evaluated the data gathered through interviews and software tools, and classified the results to identify patterns of vulnerabilities and their potential impacts on EDIS security.

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-HH-022

December 22, 2010

MEMORANDUM

TO: Philip M. Heneghan, Inspector General

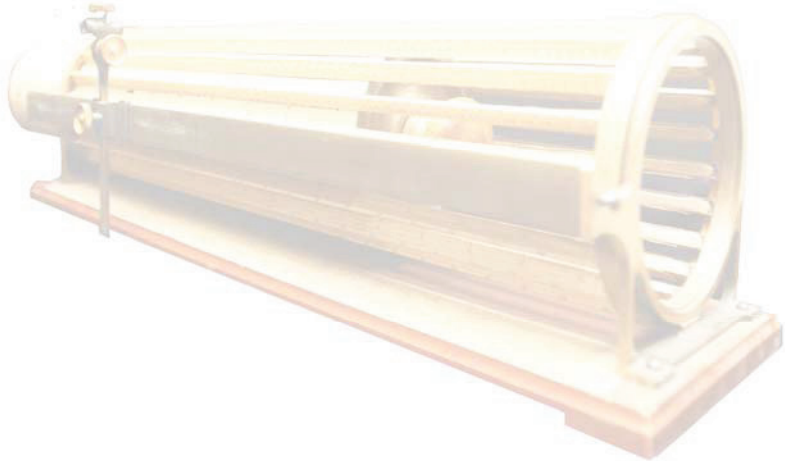
FROM: Deanna Tanner Okun, Chairman

SUBJECT: Management Response to the Inspector General's Draft Audit Report, "Audit of EDIS Security"

I am in receipt of the Inspector General's draft report, *Audit of EDIS Security*, dated November 24, 2010. I appreciate the opportunity to review the draft report and to provide comments.

The Inspector General's draft report identified four problem areas related to the security of the EDIS web application. I concur with your assessment and appreciate that your office identified 1) the agency's policy for patching ITCNet workstations was not applied to the EDIS workstations; 2) obsolete versions of software applications were installed; 3) workstations retained Internet access not required for their business functions; and 4) one workstation was configured for automatic logon of an administrative account. Management of the operational security of the Commission's critical applications is among the highest of CIO priorities, and as you found, the agency has not addressed some significant vulnerabilities in components of the EDIS web application.

Based on the finding in the draft report, the Commission has undertaken a number of immediate corrective actions to resolve or mitigate the problems you identified. Thank you for reviewing the security of EDIS and making recommendations to strengthen its effectiveness.



“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