U.S. International Trade Commission

Audit of Account Management

OIG-AR-11-11

June 29, 2011

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

OFFICE OF INSPECTOR GENERAL

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

VIA ELECTRONIC TRANSMISSION

June 29, 2011 OIG-JJ-008

Chairman Okun:

This memorandum transmits the Office of Inspector General's final report Audit of Account Management OIG-AR-11-11. 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 M. Heneghan
Inspector General

Table of Contents

Results of Audit **1**

Areas for Improvement **2**

Area for Improvement 1: Data owners should maintain permissions to restrict access to data. 2

Area for Improvement 2: Consistently configure network accounts for contractors..... 3

Area for Improvement 3: Reduce the number of authentication systems in use. 4

Management Comments and Our Analysis **5**

Objective, Scope, and Methodology **5**

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

Results of Audit

The purpose of the audit was to answer the question:

> Does the Commission effectively limit network access?

Yes, the Commission effectively limits network access.

Organizations control access to data by limiting network access, typically by requiring the use of credentials that include something the user knows, such as a user name and a password. Organizations with stronger authentication requirements also require something users physically possess, such as an authentication device or Personal Identity Verification (PIV) card. When this information is entered into a system, an authentication system checks to see that an account with the user name exists, is enabled, and verifies the password. Once authenticated, the login process is allowed to continue, and the user receives access to the data they have been permitted to modify and view. Preventing access to the network by unauthorized users is the most important component of an account management program. The Commission prevented unauthorized access by:

1. Immediately disabling accounts when users are no longer authorized to access the network;
2. Requiring the use of a hardware device, a PIN, an active user account and a strong password to access the network externally; and
3. Requiring physical identification, an active user account and a password to access the network internally.

Enabled accounts allow access to the network. When users leave, these accounts should be immediately disabled to prevent unauthorized access to the network. On January 13, 2011, we performed an analysis of user accounts on the ITCNet domain, and found that no user accounts were improperly enabled. The Commission has done an effective job of removing this important means of unauthorized network access.

While the Commission effectively prevents unauthorized network access, we have identified some areas where it can further improve its security controls concerning users that are authorized to access the network. These areas include maintenance of permissions to better restrict access to data, improved consistency of contractor account data, and consolidation of authentication systems.

Areas for Improvement

Area for Improvement 1:
Data owners should maintain permissions to restrict access to data.

Commission staff and contractors access data using a variety of means, primarily through the use of intranet sites and mapped network drives. Much of this data is grouped by office, where staff in those offices work on data specific to that office. In many offices, such as Human Resources, Finance, and Investigations, the permissions granted are intended to make data accessible only to the staff of those offices.

We analyzed the permissions assigned to two users that had been recently reassigned to new, permanent positions in the Commission. We found that their permissions reflected the needs of their current positions, but also inappropriately provided them with office-specific access required by their previous positions.

Because permissions are typically discovered using technical tools, the owners of data may not know or control who retains access to their data. Over time, as employees are reassigned to other roles within the organization, their permissions need to be updated to reflect these new roles. If permissions are not kept up-to-date, they become a historical record of all users or accounts that ever had access to that data, instead of identifying who currently has access to the data. Our analysis of the Commission's shared files and folders identified 260,545 variations in permissions for shared data, a large number, for an organization with less than 500 users. The Commission places the responsibility for maintaining these permissions on the Chief Information Officer (CIO), but only the owners of data actually know who should have access.

The maintenance of correct permissions requires a concerted effort by the functions of contracts, human resources, personnel security, and program offices to provide the CIO with status updates as they relate to accounts and their access to data. For example, when an employee is detailed or reassigned, the new program office must notify the CIO that the employee has new responsibilities which require new permissions, and the original program office must define the permissions no longer required. If this process is not implemented, users will retain access to data that their jobs do not require, and the Commission's data will be subject to unnecessary risk.

To maintain correct permissions for access to Commission data, the CIO should periodically provide clear reports to data owners detailing who has access to their data, and assist in the maintenance of these permissions.

Recommendation 1:

That the Commission develop and implement a program to have the functions of

contracts, human resources, personnel security, program, and other administrative offices notify the CIO when employee or contractor assignment status changes require the enabling or disabling of permissions.

Recommendation 2:

That the Commission identify the owner of all office and division-specific data.

Recommendation 3:

That the CIO perform a one-time cleanup of file and folder permissions.

Recommendation 4:

That the CIO provide a periodic listing of permissions to data owners.

Recommendation 5:

That the data owners review permissions on a periodic basis to verify that all users with access are authorized.

Area for Improvement 2:
Consistently configure network accounts for contractors.

The Commission identifies contractor accounts through several means, such as including "(Contractor)" in the account description, and through membership in a special "Contractors" group. It also sets an automatic expiration date for these accounts that is tied to the final day of the contract. These conditions allow contractor accounts to be quickly recognized and insures that access to the network does not extend beyond the contract expiration date.

While analyzing contractor accounts, we found:

- Some members identified in the "Contractors" group were in fact employees;
- Contractors were not always identified in the account description or through contractor group membership; and
- Some contractor accounts were missing the expiration date associated with their contract.

The Commission has not consistently implemented its procedures to identify Contractor accounts. Because of this, it is difficult to identify Contractor accounts, increasing the risk that these accounts might not be quickly disabled upon contract expiration.

Recommendation 6:

That the CIO update all contractor accounts to consistently identify these accounts and their contract expiration dates.

Area for Improvement 3:
Reduce the number of authentication systems in use.

Authentication systems make it possible to have one username and password to access multiple systems, including workstations, fileservers, and email services. Centralized authentication systems eliminate the need for users to remember and maintain multiple accounts and passwords, and reduce the labor required to manage user accounts.

The CIO has effectively limited the number of authentication systems for standard users of workstations and servers in the Active Directory domain; however, the CIO has not implemented a centralized authentication system for many servers or network infrastructure devices. Currently, each of these devices maintains its own authentication infrastructure, resulting in redundant user accounts, passwords, and inefficient account management.

Recommendation 7:

That the CIO identify all authentication systems in use within the Commission.

Recommendation 8:

That the CIO evaluate opportunities to reduce the number of authentication systems in use.

Management Comments and Our Analysis

On June 21, 2011, Chairman Deanna Tanner Okun provided management comments on the draft audit report. The Chairman agreed with our assessment that the Commission is effectively limiting network access, and recognized that the Commission can further enhance its security by implementing the recommendations detailed in the three areas for improvement. The Chairman's response is provided in its entirety as Appendix A.

Objective, Scope, and Methodology

Objective:

Does the Commission effectively limit network access?

Scope:

On January 13, 2011, we audited the enabled accounts on ITCNet. Operational staff provided us with the account policies and listings of enabled accounts for a range of other infrastructure devices including servers, RSA authentication, and permissions for domain users of shared drives.

Methodology:

a. Collect and analyze enabled accounts on the ITC domain.
b. Collect data for users of systems not authenticated by the ITC domain.
c. Analyze logs for secondary authentication systems (hardware tokens for remote access).
d. Assess and attempt to quantify different authentication systems in use.
e. Analyze permissions for commonly used file shares.
f. Identify user permissions unrelated to current job functions.

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-034

June 21, 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 Account Management"

I am in receipt of the Inspector General's draft report, *Audit of Account Management*, dated May 24, 2011. I appreciate the opportunity to review the draft report and to provide a response to the findings.

The Inspector General's draft report found that the Commission effectively limits network access. The report, however, did reveal three areas for improvement: (1) the Commission should develop and implement a program to have the functions of contracts, human resources, personnel security, and program offices notify the Office of the Chief Information Officer when employee or contractor assignment status changes require the enabling or disabling of permissions, (2) the Commission should configure network accounts for contractors in a consistent manner, and (3) the Commission should reduce the number of authentication systems in use

We agree with the findings. The Commission is dedicated to ensuring that it effectively limits network access. Thank you for reviewing the Commission's account management system and making the recommendations to strengthen its security controls concerning users that are authorized to access the network.

"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