OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Department of Commerce

Information Technology Security Controls

As of January 2011

April 15, 2011 **Report 11-08**

FINANCIAL AUDIT DIVISION
Centennial Building – Suite 140
658 Cedar Street – Saint Paul, MN 55155
Telephone: 651-296-4708 • Fax: 651-296-4712
E-mail: auditor@state.mn.us • Web site: http://www.auditor.leg.state.mn.us
Through Minnesota Relay: 1-800-627-3529 or 7-1-1

OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

April 15, 2011

Representative Michael Beard, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Michael Rothman, Commissioner
Department of Commerce

This report presents the results of our audit of the Department of Commerce's security controls that help to protect the department's computer systems and data from external threats. This report contains five findings presented in the accompanying section of this report titled, *Findings and Recommendations*.

We discussed the results of the audit with the department's staff on March 31, 2011. Management's response to our findings and recommendations are presented in the accompanying section of this report titled, *Agency Response.*

The audit was conducted by Carolyn Engstrom, CISA, CISSP (Audit Manager) and Bill Betthauser, CISA (Auditor-in-Charge).

We received the full cooperation of the Department of Commerce's staff while performing this audit.

James R. Nobles
Legislative Auditor

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

Room 140 Centennial Building, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651-296-4708 • Fax: 651-296-4712
E-mail: auditor@state.mn.us • Web Site: www.auditor.leg.state.mn.us • Through Minnesota Relay: 1-800-627-3529 or 7-1-1

Table of Contents

Page

Report Summary 1

Overview 3

Objective, Scope, and Methodology 3

Conclusion 4

Findings and Recommendations 5

1. The Department of Commerce did not develop a comprehensive security management program 5

2. The Department of Commerce had many firewall rules that were too permissive or unnecessary 6

3. The Department of Commerce did not sufficiently restrict or filter computer traffic nor did it encrypt some sensitive computer traffic in its private internal network 6

4. The Department of Commerce had not implemented formal change management processes to ensure that it adequately documented, assessed, tested, and approved proposed changes before implementing those changes in the technology environment 7

5. The Department of Commerce lacked a periodic review of some users with remote access privileges 8

Agency Response 9

Report Summary

Conclusion

The Department of Commerce did not have adequate security controls to protect the confidentiality, integrity, and availability of its data and computer systems from threats originating outside its internal network. We identified five weaknesses in internal controls.

Findings

- The Department of Commerce did not develop a comprehensive security management program. (Finding 1, page 5)

- The Department of Commerce had many firewall rules that were too permissive or unnecessary. (Finding 2, page 6)

- The Department of Commerce did not sufficiently restrict or filter computer traffic nor did it encrypt some sensitive computer traffic in its private internal network. (Finding 3, page 6)

- The Department of Commerce had not implemented formal change management processes to ensure that it adequately documented, assessed, tested, and approved proposed changes before implementing those changes in the technology environment. (Finding 4, page 7)

- The Department of Commerce lacked a periodic review of some users with remote access privileges. (Finding 5, page 8)

Audit Objective and Scope

The audit objective was to answer the following question:

- Did the Department of Commerce have adequate security controls to protect the department's computer systems and data from threats originating outside the internal network?

We assessed controls as of January 2011.

Department of Commerce

Information Technology Security Controls

Overview

The Department of Commerce regulates financial institutions, insurance, real estate, utilities, and other commercial activities, such as registration of securities and business franchises and pricing for gasoline and cigarettes. During fiscal year 2009, the department had approximately 316 full-time equivalents and spent over $291 million, derived from various funding sources. For fiscal year 2009, the department received an appropriation from the General Fund of approximately $22 million, while also receiving money from the Petroleum Tank Release Cleanup Fund and the Workers' Compensation Fund.[1]

The information technology group resides within the Administration Division of Commerce. It employs about 12 individuals and is responsible for the department's information technology services, including day-to-day management of the department's network and servers, consisting of approximately 550 devices.

Objective, Scope, and Methodology

The audit objective was to answer the following question:

- Did the Department of Commerce have adequate security controls to protect the department's computer systems and data from threats originating outside the internal network?

To answer this question, we interviewed department staff and reviewed relevant documentation. We also used a variety of computer-assisted auditing tools and other techniques to analyze the security infrastructure and test controls. We assessed controls as of January 2011.

The audit focused on the department's controls that protected its data from unauthorized disclosure and modification resulting from external threats, such as hackers, or threats that result from internal users accessing external malicious resources. Organizations often implement controls at multiple layers of a computer network so that if one control fails, other controls will mitigate the risk of compromise. Examples of controls reviewed include network design, firewall management, patch management, anti-virus and anti-malware software scanning, and vulnerability and threat management.

[1] State of Minnesota Biennial Budget 2010-11.

We conducted this audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. To assess security controls, we used criteria contained in *Special Publication 800-53, Recommended Security Controls for Federal Information Systems*, published by the National Institute of Standards and Technology's Computer Security Division. We also used criteria contained in security guidance, published by the Defense Information Systems Agency, and information published by applicable technology vendors to evaluate select controls. When available, we also used department and state policies to obtain evaluation criteria.

Conclusion

The Department of Commerce did not have adequate security controls to protect the confidentiality, integrity, and availability of its data and computer systems from threats originating outside its internal network. We identified five weaknesses in internal controls.

The following *Findings and Recommendations* section explains the weaknesses.

Findings and Recommendations

Finding 1

The Department of Commerce did not develop a comprehensive security management program.

The department did not develop a comprehensive security management program.[2] A comprehensive security management program is a formal method used by an organization to effectively identify and manage risks throughout an organization and promptly respond to changing threats. Not unlike other important business functions, such as accounting and finance, the organization should establish the responsibility and authority for system security at its highest levels. The security program should be well managed and include proper planning and oversight activities. Without a comprehensive security program, the department will likely be unable to effectively and proactively manage information technology risks and security.

Risk assessments and policies and procedures are key components of a security management program. The department had conducted some informal assessments but had not adopted and implemented a formal methodology to evaluate risks. Risk assessment methodologies provide a framework for consistently identifying, quantifying, and prioritizing risks related to information assets. The results help management understand factors that can negatively influence operations and assist in making informed decisions regarding the implementation of selected controls. The results also aid the department in developing and maintaining effective information security plans. If periodic risk assessments are not performed, risk to the organization could continue, unidentified and unmitigated, until the risk is realized.

The department had drafted some information technology policies but had not finalized and approved them yet. While the Office of Enterprise Technology has authority to establish strategic policies across state agencies, individual agencies have the responsibility, under the Office of Enterprise Technology's Enterprise Security Program Policy, to "develop and maintain additional policies and standards to address entity specific regulatory requirements or other needs." Without formal policies, standards, or procedures from the department's management, information technology staff had little guidance in performing their day-to-day tasks.

Recommendations

- *The department should develop a comprehensive security management program.*

[2] The National Institute of Standards and Technology developed special publications that provide guidance on planning, implementing, and managing an ongoing security management program.

- *The department should adopt a risk assessment methodology and perform periodic assessments.*

- *The department should complete the development of written security policies, standards, and procedures and monitor compliance with them.*

Finding 2

The Department of Commerce had many firewall rules that were too permissive or unnecessary.

Many of the department's firewall rules either allowed excessive access or were no longer needed. The department had not adequately documented the business justification or purpose for the rules nor did it implement monitoring procedures, which could have helped identify unnecessary rules more easily. The department lacked formal firewall rule change procedures that required requests for new rules or modification of existing rules be documented, reviewed, and approved by appropriate staff. The department also had not periodically reviewed and recertified the rules to ensure they were appropriate.

A poorly managed firewall increases the risk that it may not be adequately defending the department against hackers and other external threats. A firewall examines all traffic that attempts to enter or leave an organization's private network. Traffic that does not meet certain conditions, defined in firewall rules, cannot pass in or out of the private network.

Recommendations

- *The department should develop formal firewall management procedures, including change management procedures that include requesting, reviewing, approving, and documenting firewall rule changes. Procedures should also include the periodic review and recertification of the firewall rules.*

- *The department should conduct a complete review of its firewall rules. It should remove unneeded rules and further restrict excessively permissive rules.*

Finding 3

The Department of Commerce did not sufficiently restrict or filter computer traffic nor did it encrypt some sensitive computer traffic in its private internal network.

The department did not adequately restrict computer traffic in its private internal network, as shown by the following examples:

- The department did not restrict computer traffic, such as voice and data, between portions or segments of its private internal network.

- The department did not sufficiently limit the ability to connect to critical devices to specifically authorized internal computers.

- The department did not exclusively use secure protocols for administering devices.

Network filtering improves controls by creating rules that only allow authorized traffic in or out of each segment on the private internal network. The risks of not having traffic restrictions is that a hacker, user, virus, or other malware that gained unauthorized access to a part of the department's internal network could attempt to move throughout the network and eavesdrop on data and voice traffic or attempt to access software and data on computers. If a portion of the network is compromised, implementing secure protocols with encryption limits the ability of an intruder to eavesdrop on the transmission of nonpublic data on the network.

Recommendations

- *The department should further segment and filter computer traffic in its private internal network.*

- *The department should restrict the ability to attempt to connect to critical devices to specifically authorized internal computers.*

- *The department should prohibit unencrypted connections from being used to administer critical devices.*

Finding 4

The Department of Commerce had not implemented formal change management processes to ensure that it adequately documented, assessed, tested, and approved proposed changes before implementing those changes in the technology environment.

The department had an informal process to assess changes to the technology environment. While staff discussed many of the changes in regular security meetings, the department did not document processes for tracking, assessing, testing, authorizing, or documenting changes.

Our testing showed that one device was missing a patch, which increased its suspectibility to certain low priority security vulnerabilities. If the department does not consistently assess system change requests, staff could make decisions that weaken the network's security or affect the availability of critical technology.

Recommendation

- *The department should implement a change management process that establishes the roles and responsibilities for assessing, testing, approving, and documenting changes to the technology environment.*

Finding 5

The Department of Commerce lacked a periodic review of some users with remote access privileges.

The department lacked a periodic review of some users with remote access to internal applications. Controls were generally adequate to ensure appropriate access for employees and insurance examiner contractors. However, the department did not have a formal process to periodically review contractors that were not insurance examiners. Granting access to contractors is risky because information technology staff may not be notified to terminate remote access in a timely manner, which would allow a contractor to continue to access the department's internal applications beyond the needed time period.

Recommendation

- *The department should implement periodic reviews of remote access privileges for all users.*

MINNESOTA
DEPARTMENT OF
COMMERCE

85 7th Place East, Suite 500
St. Paul, Minnesota 55101-3165
www.commerce.state.mn.us
651.296.4026 FAX 651.297.1959
An equal opportunity employer

April 8, 2011

James R. Nobles
Legislative Auditor
Office of the Legislative Auditor
Centennial Office Building, Room 140
658 Cedar Street
St. Paul, MN 55155-1603

Dear Mr. Nobles:

I would like to thank the Office of the Legislative Auditor and your information technology team for the work on the recent audit of select information security controls at the Minnesota Department of Commerce. Your team has provided a professional review of controls on the Department's systems and valuable recommendations for improving its security posture. I welcome the opportunity to take positive action on their recommendations. We agree with the overall findings of the audit.

In my role as a new Commissioner at the Commerce Department, I am committed to effective internal controls, including security measures that protect the confidentiality, integrity, and availability of our computer systems. The findings and associated recommendations will augment our ongoing efforts to safeguard our information assets and the supporting infrastructure.

Specific responses to the audit findings follow.

Finding 1: The Department of Commerce did not develop a comprehensive security management program.

Recommendations:

- *The department should develop a comprehensive security management program.*
- *The department should adopt a risk assessment methodology and perform periodic assessments.*
- *The department should complete the development of written security policies, standards, and procedures and monitor compliance with them.*

Response: The Department agrees with the finding and will develop a formal, comprehensive security program. We will address policies, milestones, risk management, and change management. Commerce's Chief Information Security Officer (Richard Gooley) and Chief Information Officer (Greg Fetter) will be primarily responsible for this development. The program will be in place by May 31, 2011.

Finding 2: The Department of Commerce had many firewall rules that were too permissive or unnecessary.

Recommendations:

- *The department should develop formal firewall management procedures, including change management procedures that include requesting, reviewing, approving, and documenting firewall rule changes. Procedures should also include the periodic review and recertification of the firewall rules.*

- *The department should conduct a complete review of its firewall rules. It should remove any unneeded rules and further restrict excessively permissive rules.*

Response: The Department agrees with the finding and has reduced its firewall rule set and instituted regular reviews. We have documented our re-designed firewall management procedures. Commerce's Chief Information Security Officer and Network Manager (Lena Messing) were primarily responsible for developing these procedures. The procedures were documented and in place as of April 7, 2011.

Finding 3: The Department of Commerce did not sufficiently restrict or filter computer traffic nor did it encrypt some sensitive computer traffic within its private internal network.

Recommendations:

- *The department should further segment and filter computer traffic in its private internal network.*

- *The department should restrict the ability to attempt to connect to critical devices to specifically authorized internal computers.*

- *The department should prohibit unencrypted connections from being used to administer critical devices.*

Response: The Department agrees with the finding and will further restrict and filter network traffic on its internal networks. Commerce's Chief Information Security Officer and Network Manager will be primarily responsible for this effort. The changes will be in place by May 31, 2011.

Finding 4: The Department of Commerce had not implemented formal change management processes to ensure that it adequately documented, assessed, tested, and approved proposed changes before implementing those changes in the technology environment.

Recommendations:

- *The department should implement a change management process that establishes the roles and responsibilities for assessing, testing, approving, and documenting changes to the technology environment.*

Response: The Department agrees with the finding and is developing a formal change management process as part of our comprehensive security program. Commerce's Chief Information Security Officer and Chief Information Officer will be primarily responsible for this development. The process will be in place by April 15, 2011.

Finding 5: The Department of Commerce lacked a periodic review of some users with remote access privileges.

Recommendation:

- *The department should implement periodic reviews of remote access privileges for all users.*

Response: The Department agrees with the finding and has instituted periodic review of remote access privileges for all users. Commerce's Chief Information Security Officer and Network Manager conduct these reviews. The second periodic review was completed on March 30, 2011.

I appreciate the work of your agency to identify areas within Commerce that need improvement. We are committed to taking appropriate action to further strengthen our security controls structure.

Sincerely,

Mike Rothman
Commissioner