OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Department of Agriculture

Network Security Controls

Information Technology Audit

July 1, 2010 **Report 10-23**

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

OLA

OFFICE OF THE LEGISLATIVE AUDITOR

State of Minnesota • James Nobles, Legislative Auditor

July 1, 2010

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Gene Hugoson, Commissioner
Minnesota Department of Agriculture

This report presents the results of our audit of the Department of Agriculture's security controls that help to protect the department's computer systems and data from external threats. This report contains four 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 June 10, 2010. 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 Eric Wion, CISA, CISSP, CPA (Audit Manager), Aimee Martin, CISA (Auditor-in-Charge), Carolyn Engstrom, CISA (Audit Coordinator), and Bill Betthauser, CISA (Senior Auditor).

This report is intended for the information and use of the Legislative Audit Commission and the management of the Department of Agriculture. This restriction is not intended to limit the distribution of this report, which was released as a public document on July 1, 2010.

James R. Nobles

James R. Nobles
Legislative Auditor

Cecile M. Ferkul

Cecile M. Ferkul, CPA, CISA
Deputy Legislative Auditor

Table of Contents

Report Summary

Conclusion

The Department of Agriculture generally had adequate security controls to protect the classifications, integrity, and availability of its data and computer systems from threats originating outside its internal network. However, we identified four weaknesses in internal controls.

Findings

- The Department of Agriculture did not conduct formal risk assessments. (Finding 1, page 5)

- The Department of Agriculture did not assess its monitoring needs nor did it proactively review some security events. (Finding 2, page 5)

- The Department of Agriculture did not sufficiently restrict or filter computer traffic in its private internal network. (Finding 3, page 6)

- The Department of Agriculture did not periodically recertify some access privileges nor did it implement strong password controls on some accounts. (Finding 4, page 7)

Audit Objective and Scope

The audit objective was to answer the following question:

- Did the Department of Agriculture have adequate security controls to protect the department’s computer systems and data from external threats?

We assessed controls as of May 2010.

Department of Agriculture

Overview

The Minnesota Department of Agriculture administers a wide range of programs that support, promote, and protect the state's agricultural sector. During fiscal year 2009, the department had approximately 350 employees and spent over $80 million derived from various funding sources. Over half of the department's resources were appropriated from the General Fund; the rest came from special appropriations, program revenues and fees, and federal grants.[1]

The department has a centralized information technology division. As of April 2010, the department had about 20 information technology staff, including a chief information security officer. Approximately five of these staff were responsible for 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 Agriculture have adequate security controls to protect the classifications, integrity, and availability of its data and computer systems from external threats?

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 May 2010.

The audit focused on the department's controls that protect 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 Agriculture generally had adequate security controls to protect the classifications, integrity, and availability of its data and computer systems from external threats. However, we identified four weaknesses in internal controls.

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

Findings and Recommendations

Finding 1

The Department of Agriculture did not conduct formal risk assessments.

The department did not periodically assess risks relevant to its computer systems and data and determine whether it had effective controls in place to address those risks. Assessments are important because they help to identify, quantify, and prioritize risks. The results help management understand factors that can negatively influence operations and make informed decisions regarding the appropriate action and priorities for managing information security risks and for implementing controls selected to protect against those risks. The results also aid in developing or maintaining effective information security policies and standards.

Recommendation

- *The department should develop risk assessment methodologies and perform periodic assessments.*

Finding 2

The Department of Agriculture did not assess its monitoring needs nor did it proactively review some security events.

The department's monitoring procedures were not sufficient to detect and appropriately respond to important security-related events, such as external attacks, unauthorized attempts to access computers or sensitive files, changes to critical computer settings, employee system misuse, and exceptions to defined policies and procedures in a timely manner.

While the department employed real-time monitoring of certain security events, the department had not formally assessed which security-related events put its systems and data at highest risk. Further, the department did not regularly and proactively review many of its security logs. It had not assigned the review of logs to specific staff or identified the frequency of reviews. The department did not have software to assist in the gathering and analyzing of security logs to identify events that require attention.

Finally, the department did not develop and implement a strategy to ensure it maintained, backed up, and archived all security log records. It is important to have historic log information available should the department or law enforcement need to conduct an investigation.

Without adequate security event monitoring procedures, the department would likely be unable to be proactive and take timely and appropriate action to protect its computer systems and data if an attack occurred.

Recommendations

- *The department should assess its monitoring needs to determine what events it needs to log, who should review the logs, and the frequency of the reviews. It should consider acquiring technologies to facilitate the systematic review and analysis of security events.*

- *The department should define and follow its records retention requirements for security log records.*

Finding 3

The Department of Agriculture did not sufficiently restrict or filter computer traffic in its private internal network.

The department did not adequately restrict computer traffic in its private internal network. For example, it did not:

- Restrict or filter computer traffic from employee computers accessing internal computers from remote locations.

- Restrict or filter computer traffic between portions or segments of its private internal network.

- Limit the ability to log into critical devices to specifically authorized internal computers belonging only to information technology staff.

Network filtering improves control by only allowing authorized traffic in or out of each segment on the private internal network. Without adequate filtering, someone who gained unauthorized access to portions of the department's private internal network could attempt to move throughout the network and access software and data on any computer. Filtering also helps to prevent the spread of malicious software, such as viruses, worms, and trojans.

Recommendation

- *The department should restrict or filter computer traffic in its private internal network.*

Finding 4

The Department of Agriculture did not periodically recertify some access privileges nor did it implement strong password controls on some accounts.

The department did not periodically review and reconfirm the need for some employees to access network devices or to remotely access the department's private internal network from outside the network. Several current and past employees with remote access had not used their accounts in over a year.[2]

The department also had several weaknesses in the use of passwords to control and limit access to its network or network devices.

- Some information technology staff shared passwords used to administer or manage critical devices. Sharing passwords prevents the department from determining employee accountability for changes made to the network.
- The department had not changed some default passwords set by vendors for purchased technologies and software. Hackers can easily find default passwords on Internet websites and use them to gain unauthorized access.
- The department had not implemented adequate password complexity requirements and account lockout controls for some accounts.

Strong password controls are important to help prevent employees and hackers from assuming the identity of legitimate system users and to enforce individual accountability.

Recommendations

- *The department should periodically review and recertify those with network device and remote access to ensure that they still require access.*
- *The department should prohibit the sharing of network passwords.*
- *The department should promptly change default and easy to guess passwords.*
- *The department should implement password complexity requirements and account lockout features.*

[2] The department had other controls that prevented past employees from remotely accessing the department's internal network.

MINNESOTA DEPARTMENT OF AGRICULTURE

June 21, 2010

Mr. Jim Nobles
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 team for the work on the information technology audit of select information security controls at the Minnesota Department of Agriculture (MDA). We value the professional review and assessment your team has provided through this audit and we appreciate the recommendations for improvement. Furthermore, we agree with your overall findings.

MDA understands the importance of providing effective security measures to protect the confidentiality, integrity, and availability of our computer systems. The four findings and associated recommendations will supplement our ongoing Information Technology Security and Risk Management Program efforts to safeguard our information assets and the supporting infrastructure against unauthorized use, disclosure, modification, damage or loss.

MDA acknowledges and recognizes that mitigation activity will take time and resources, and require technical sophistication. Specific Responses to this audit follow.

Finding 1: The Department of Agriculture did not conduct formal risk assessments.

Recommendations:

- *The department should develop risk assessment methodologies and perform periodic assessments.*

Response: The department agrees with the finding and recommendation. MDA will begin to formalize its risk assessment program and process by examining and evaluating risk assessment strategies and methodologies. MDA will develop a project plan and budget to address this finding by January 31, 2011. MDA's Chief Information Officer and Chief Information Security Officer will be responsible for this task.

Finding 2: The Department of Agriculture did not assess its monitoring needs nor did it proactively review some security events.

Recommendations:

- *The department should assess its monitoring needs to determine what events it needs to log, who should review the logs, and the frequency of the reviews. It should consider acquiring technologies to facilitate the systematic review and analysis of security events.*

- *The department should define and follow its records retention requirements for security log records.*

Response: The department agrees with the finding and recommendations. Prior to the issuance of this audit report, MDA was assessing monitoring needs and evaluating available technology to assist in the management and analysis of logs and security events. MDA will continue with its efforts to address this finding and analyze risk factors and business impacts. The Information Technology Assistant Division Director and Chief Information Security Officer will oversee the resolution of this finding by December 31, 2010.

The MDA will evaluate legal and business requirements in determining the type of system logs and management procedures needed for establishment of record retention requirements.   The Chief Information Officer will oversee the resolution of this finding by November 1, 2010.

Finding 3: The Department of Agriculture did not sufficiently restrict or filter computer traffic in its private internal network.

Recommendations:

- *The department should restrict or filter computer traffic in its private internal network.*

Response: The department agrees with the finding and recommendation. The department will create a project plan and institute measures to mitigate this finding by December 31, 2010. The Information Technology Division Assistant Director and Chief Information Security Officer will oversee the response.

Finding 4: The Department of Agriculture did not periodically recertify some access privileges nor did it implement strong password controls on some accounts.

Recommendations:

- *The department should periodically review and recertify those with network device and remote access to ensure that they still require access.*

- *The department should prohibit the sharing of network passwords.*

- *The department should promptly change default and easy to guess passwords.*

- *The department should implement password complexity requirements and account lockout features.*

Response: The department agrees with the finding and recommendation. The MDA will review existing policies and procedures, making necessary modifications and amendments to periodically review access privileges. Measures are already in process to mitigate sharing of network passwords, remove identified default password, and put into operation password complexity requirements. The Information Technology Assistant Division Director and Chief Information Security Officer will oversee the resolution of this finding. Policy and procedures recommendations will be completed by October 31, 2010 while other steps will be completed by July 31, 2010.

Sincerely,

Gene Hugoson

Gene Hugoson
Commissioner