OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Department of Management and Budget and the Office of Enterprise Technology

State Personnel and Payroll System Security Controls

Information Technology Audit

February 11, 2010 **Report 10-02**

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

Financial Audit Division

The Financial Audit Division annually audits the state's financial statements and, on a rotating schedule, audits agencies in the executive and judicial branches of state government, three metropolitan agencies, and several "semi-state" organizations. The division has a staff of forty auditors, most of whom are CPAs. The division conducts audits in accordance with standards established by the American Institute of Certified Public Accountants and the Comptroller General of the United States.

The Office of the Legislative Auditor (OLA) also has a Program Evaluation Division, which evaluates topics periodically selected by the Legislative Audit Commission.

Reports issued by both OLA divisions are solely the responsibility of OLA and may not reflect the views of the Legislative Audit Commission, its individual members, or other members of the Minnesota Legislature. For more information about OLA reports, go to:

http://www.auditor.leg.state.mn.us

To obtain reports in electronic ASCII text, Braille, large print, or audio, call 651-296-4708. People with hearing or speech disabilities may call through Minnesota Relay by dialing 7-1-1 or 1-800-627-3529.

To offer comments about our work or suggest an audit, investigation, or evaluation, call 651-296-4708 or e-mail auditor@state.mn.us.

OLA

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

February 11, 2010

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Tom Hanson, Commissioner
Department of Management and Budget

Mr. Gopal Khanna, State Chief Information Officer
Office of Enterprise Technology

This report presents the results of our audit of the Department of Management and Budget and the Office of Enterprise Technology's security controls that help to protect the integrity, confidentiality, and availability of the state's personnel and payroll system and data. This report contains six findings presented in the accompanying section of this report titled, *Findings and Recommendations*.

We discussed the results of the audit with the Department of Management and Budget and the Office of Enterprise Technology's staff on February 2, 2010. Management's response to our findings and recommendations are presented in the accompanying section of this report titled, *Agencies Responses.*

The audit was conducted by Eric Wion (Audit Manager), Aimee Martin (Auditor-in-Charge), Bill Betthauser (Senior Auditor), and John Kelcher (Senior Auditor).

/s/ James R. Nobles	*/s/ Cecile M. Ferkul*
James R. Nobles Legislative Auditor	Cecile M. Ferkul, CPA, CISA Deputy Legislative Auditor

Table of Contents

Report Summary

Conclusion

The Department of Management and Budget and the Office of Enterprise Technology generally had adequate security controls for the state's personnel and payroll system and its data. However, the agencies lacked some important security controls.

The Department of Management and Budget resolved the prior eight audit findings applicable to the scope of this audit.

Key Findings

- The Department of Management and Budget did not conduct formal risk assessments nor develop adequate written information security policies, standards, and procedures. (Finding 1, page 5)
- The Department of Management and Budget did not have adequate controls to ensure some computer users' access was appropriate on an ongoing basis. (Finding 2, page 5)
- The Department of Management and Budget had not formalized how it would detect, monitor, and resolve computer vulnerabilities and did not promptly install updates and patches on some of its computers. (Finding 3, page 6)
- The Department of Management and Budget did not have effective monitoring procedures to detect and promptly respond to security-related events. (Finding 4, page 7)

Audit Objective and Scope

The audit objective was to answer the following questions:

- Did the Department of Management and Budget and the Office of Enterprise Technology have adequate security controls to protect the confidentiality, integrity, and availability of the state's personnel and payroll system and its business data?
- Did the Department of Management and Budget resolve prior audit findings?

We assessed controls as of October 2009.

Department of Management and Budget and the Office of Enterprise Technology

State Personnel and Payroll System: State Employee Management System

Overview

The Department of Management and Budget is responsible for managing and providing leadership in financial management, human resources, and enterprise systems and analysis. One of its core functions is managing the state's personnel and payroll system, called the State Employee Management System.[1]

Over 45,000 employees use the state's web-based personnel and payroll system. Most state agencies use the system to process personnel and payroll transactions. Many state agencies allow employees to electronically enter timesheet information and supervisors to electronically approve the time worked. Employees use the system to view their paychecks, leave balances, benefits, and make changes to benefits during open enrollment periods.

The Department of Management and Budget's information technology unit manages its computing environment, including many aspects of the state's personnel and payroll system. The department contracted with the Office of Enterprise Technology to provide data center space, hardware, and other information system services. Each organization is responsible for key security controls.

Objective, Scope, and Methodology

The audit objective was to answer the following questions:

- Did the Department of Management and Budget and the Office of Enterprise Technology have adequate security controls to protect the confidentiality, integrity, and availability of the state's personnel and payroll system and its business data?

[1] The state commonly refers to this system as SEMA4.

- Did the Department of Management and Budget resolve prior audit findings?[2]

To answer these questions, we interviewed staff of the Department of Management and Budget and the Office of Enterprise Technology. We reviewed policies, procedures, and other 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 October 2009.

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 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

We concluded that the Department of Management and Budget and the Office of Enterprise Technology generally had adequate security controls to protect the integrity, confidentiality, and availability of the state's personnel and payroll system and its data. However, as highlighted in the next section, the agencies lacked some important security controls.

The Department of Management and Budget resolved the prior eight audit findings applicable to the scope of this audit.

The following *Findings and Recommendations* section explains the deficiencies. The Department of Management and Budget is responsible for resolving the findings; however, the department will likely need to coordinate remediation efforts with the Office of Enterprise Technology since it also helps manage some of the day-to-day tasks that help support the ongoing operation of the state's personnel and payroll system.

[2] Findings 4 through 6, Office of the Legislative Auditor, Financial Audit Division Report 07-01, *SEMA4 Personnel and Payroll Controls*, issued January 23, 2007, and Findings 1 through 5, Report 04-36, *SEMA4 Information Technology Audit,* issued August 31, 2004.

Findings and Recommendations

Finding 1

The Department of Management and Budget did not conduct formal risk assessments nor develop adequate written information security policies, standards, and procedures.

The department did not conduct formal risk assessments, which provide decision makers with information needed to understand factors that can negatively influence operations, allowing them to make informed judgments concerning the extent of actions needed to reduce risk. The results of these assessments also would help the department design policies, standards, and procedures to reduce risks to a level management is willing to accept.

Although the department had some written policies, it lacked several important policies, standards, and procedures addressing information technology risks and security. These are critical because they outline management's security expectations. They also help define employees' roles and responsibilities. Employees cannot make consistent security decisions without policies and standards to refer to as guidance. Had the department proactively defined and communicated its security expectations, it may have averted the findings in this report.

Recommendations

- *The Department of Management and Budget should develop risk assessment methodologies and perform periodic assessments.*

- *The Department of Management and Budget should further develop written security policies, standards, and procedures and monitor compliance with them.*

Finding 2

The Department of Management and Budget did not have adequate controls to ensure some computer users' access was appropriate on an ongoing basis.

The department did not have adequate controls to ensure computer users' access to critical resources, including computers that are part of the state's personnel and payroll system, its database, and sensitive data files, was appropriate on an ongoing basis. More specifically, the department lacked formal processes to request, review, authorize, and periodically recertify people's access.

Some department and Office of Enterprise Technology staff had inappropriate or excessive access, and the department lacked controls to monitor their actions.

- About 140 people and software programs had the ability to read sensitive data files and about 100 of those, Office of Enterprise Technology staff and software programs, had the ability to modify the files. Some sensitive files contained not public data about employees, including employees' bank account information used for direct deposit.

- Four people had the ability to create accounts and assign or modify the system access given to them.

- 19 people, including 15 software developers, had the ability to change any personnel and payroll system data through the application.

- 13 people had access to the personnel and payroll system's database that no longer needed it.

The ability to read and modify sensitive files used in banking and other processes should be limited to few people, and the department should monitor their actions.

Recommendations

- *The Department of Management and Budget should develop formal procedures for requesting, reviewing, and authorizing access to personnel and payroll system related computers, databases, and sensitive files.*

- *The Department of Management and Budget should develop procedures to periodically review and recertify people's access to personnel and payroll system related computers, databases, and sensitive files.*

- *The Department of Management and Budget should further restrict who can access not public data and monitor actions performed on sensitive files.*

Finding 3

The Department of Management and Budget had not formalized how it would detect, monitor, and resolve computer vulnerabilities and did not promptly install updates and patches on some of its computers.

The department did not have processes in place to identify and resolve computer vulnerabilities in a timely manner. Although the Office of Enterprise Technology used an Enterprise Vulnerability Management System to conduct monthly external scans of Internet-accessible computers to identify vulnerabilities, the department did not routinely scan computers that are part of the state's personnel and payroll system and accessible from inside the department. Had the department performed periodic scans, it would have learned some computers had serious security vulnerabilities. For example, several computers were running insecure software because the department had not installed security-related software updates or patches.

The department uses many commercial software packages. Computer hackers routinely discover and exploit flaws or vulnerabilities in commercial software to gain unauthorized access to computer systems. When these exploits occur, vendors develop and publish software patches to correct the deficiencies in their products. Organizations that do not promptly install these software patches make their systems easy targets for computer hackers. State policy requires each agency to manage and monitor their computers for vulnerabilities and implement and maintain vulnerability remediation processes.[3]

Recommendations

- *The Department of Management and Budget should develop a formal vulnerability and threat management program to ensure it routinely scans computers and corrects critical vulnerabilities in a timely manner.*

- *The Department of Management and Budget should develop procedures to ensure it installs security-related software updates or patches in a timely manner.*

Finding 4

The Department of Management and Budget did not have effective monitoring procedures to detect and promptly respond to security-related events.

The department's monitoring procedures were not sufficient to detect and appropriately respond to important security-related events on computers that are part of the state's personnel and payroll system, such as potential external attacks, unauthorized attempts to access computers, employee system misuse, changes to critical computer settings, access to sensitive files, and exceptions to defined policies and procedures.

The department's monitoring efforts were not effective because it had not assessed which security-related events put the system at highest risk and had not customized its computers to log those high-risk events. The logs for some of the department's computers included all security-related events, while other logs did not include some rudimentary, but critical, security events. Department staff was not regularly and proactively reviewing security events. The department had not

[3] *Office of Enterprise Technology: Enterprise Security Vulnerability Management Policy 2008-04.*

assigned the review of logs to specific staff, identified how often they should review the logs, and identified what would be considered suspicious activity and the action they should take in response to suspicious activity. The department did not have software to assist in the gathering and analyzing of security logs to identify events that require attention.

Recommendation

- *The Department of Management and Budget should assess its monitoring needs to determine what events it needs to log, who should review the logs, the frequency of the review, and procedures for incident response. It should consider acquiring technologies to facilitate the systematic review and analysis of security events.*

Finding 5

The Department of Management and Budget lacked formal procedures for requesting, reviewing, approving, documenting, and periodically recertifying firewall rules, and some rules were too permissive.

The department lacked formal firewall rule change processes that included request, review, approval, and documentation of rule changes. The department lacked documentation of the business purpose of the rules and had not periodically reviewed the rules to ensure they were appropriate. Without adequate documentation, staff was not sure about the purpose of some rules. A few of the rules were no longer needed, and others were too permissive.

A firewall is typically an organization's first line of defense against external threats from hackers. A firewall is a computer that separates an organizations private internal network from the public Internet. Serving as gatekeeper, 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. Poor change controls and lack of periodic reviews often result in firewall rules that are outdated or too permissive.

Recommendation

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

Finding 6

The Department of Management and Budget did not consistently enforce strong password controls.

The department did not use customizable features to consistently enforce strong password controls across its computers.[4] While the department provided a tool and encouraged staff to select strong passwords, the department did not enforce strong controls by setting customizable computer features to, for example, prevent employees from selecting easy to guess passwords, like dictionary words, and to require that employees periodically change their passwords. The department could also use customizable features to disable accounts employees had not used for prolonged periods or that had repeated failed logon attempts, which might be an indication of someone trying to get unauthorized access. We examined these and other password settings and found they were inconsistently applied on different computers, and some settings were weak.

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

Recommendation

- *The Department of Management and Budget should define its password-related requirements, implement, and enforce strong password controls.*

[4] This control weakness did not apply to users of the application.

MINNESOTA
Management
& Budget

February 8, 2010

James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
140 Centennial Office Building
658 Cedar Street
St. Paul, Minnesota 55155

RE: OLA Audit: Information Technology Audit – SEMA4

Dear Mr. Nobles:

Thank you for the opportunity for our staff to discuss your audit findings with the individuals in your office responsible for the State Personnel and Payroll System (SEMA4) Security Controls audit. We are committed to providing secure access to accurate, timely data to state agencies. We also appreciate the written and verbal reviews by the team that performed this work from your office.

We appreciate and agree with the conclusion of your report: "*We concluded that the Department of Management and Budget and the Office of Enterprise Technology generally had adequate security controls to protect the integrity, confidentiality, and availability of the state's personnel and payroll system and its data.*" We also agree with you that improvements can be made. We appreciate your recommendations and will continue to place emphasis on security practices.

We know that security is an area where there is always the potential to do more. The challenges are ever changing. We remain committed to providing excellent security and we will continue to work toward improvements in our processes and our documentation. Your recommendations are useful to accomplishing that goal. Together, with the Office of Enterprise Technology, we will address these findings and recommendations. A brief response for each finding, including who will be responsible for the corrective actions, is provided in the following:

Recommendation

Finding 1. The Department of Management and Budget should develop risk assessment methodologies and perform periodic assessments. The Department of Management and Budget should further develop written security policies, standards, and procedures and monitor compliance with them.

Response

We agree with the recommendations. While Minnesota Management & Budget (MMB) practices sound security controls and processes and makes regular management level risk assessment decisions about where to focus and apply mitigation strategies, these processes and decisions are not always well documented. In our exit conference, we were in agreement with your staff and the Office of Enterprise Technology (OET) that these recommendations will require significant amounts of technical and business manager time to implement. As OET implements enterprise-wide security policies and standards, we will utilize these to further our efforts. Until these policies and standards are implemented for the enterprise, MMB will formulate policies and standards which will address the recommendations above. MMB will develop a strategic security system charter and policies, including risk assessment methodologies. We will work with the agency's Internal Control unit to develop an effective risk management framework. A multi-year plan for developing and implementing these policies and procedures will be created. These steps will be part of this effort:

- Adopt a risk assessment methodology
- Develop the necessary written security policies, standards, and procedures
- Perform an initial risk assessment
- Develop and implement changes as a result of the risk assessment decisions

Person responsible: Ron Olsen, Chief Security Officer, MMB

Implementation date: Develop plans and select a methodology by July 2010; date for completion of the risk assessment and full implementation of the recommendations to be determined at that time.

Recommendation

Finding 2**.** The Department of Management and Budget should develop formal procedures for requesting, reviewing, and authorizing access to personnel and payroll system related computers, databases, and sensitive files. The Department of Management and Budget should develop procedures to periodically review and recertify people's access to personnel and payroll system related computers, databases, and sensitive files. The Department of Management and Budget should further restrict who can access not public data and monitor actions performed on sensitive files.

Response

We agree with the recommendations. These recommendations have been and continue to be in place for all our users. Your recommendations are to apply similar processes for internal, central support staff. We agree this should be done. We have begun to implement internal annual re-certification for MMB staff. We will continue to work with OET to reduce the number of OET individuals required to have clearance to our systems and data to only those determined to be essential to the process. We will certify at least annually the access of our support staff and will place risk mitigation controls around the more sensitive files, including monitoring actions, as recommended. We have already begun to institute a process for the first recommendation above and the other recommendations will follow soon.

Persons responsible: MMB managers: Laurie Hansen, HRM Division Director,
John Vanderwerf, Chief Technology Officer, working with
OET management

Implementation date: June 2010

Recommendation

Finding 3. The Department of Management and Budget should develop a formal vulnerability and threat management program to ensure it routinely scans computers and corrects critical vulnerabilities in a timely manner. The Department of Management and Budget should develop procedures to ensure it installs security-related software updates or patches in a timely manner.

Response

We agree with the recommendations. While we do have most of these procedures in place for patches, we agree that even more complete procedures should be implemented. As indicated in response to Finding 1, we will further develop our documentation on policies and procedures. Regular scanning for most systems has been in place for several years. We have added the remainder of the critical production systems and will ensure that all important systems are included.

Person responsible: Ron Olsen, Chief Security Officer
John Vanderwerf, Chief Technology Officer

Implementation date: Mitigation of this finding by July 2010; date of full implementation of the vulnerability management program to be determined as part of plans referenced in Response 1 above.

Recommendation

Finding 4. The Department of Management and Budget should assess its monitoring needs to determine what events it needs to log, who should review the logs, the frequency of the review, and procedures for incident response. It should consider acquiring technologies to facilitate the systematic review and analysis of security events.

Response

We agree with the recommendation that we should assess our monitoring needs more formally. We will work with the Office of Enterprise Technology to assess logging and monitoring needs and potential software solutions and costs. We will continue to strike a balance between costs and perceived risks. As part of the plans referenced in Response 1 above, monitoring will be considered as part of the risk assessment/risk mitigation plans.

Person responsible: John Vanderwerf, Chief Technology Officer and OET representatives

Implementation date: October 2010 for assessment of monitoring needs, costs, and OET software solutions.

Recommendation

Finding 5. The Department of Management and Budget should develop formal firewall change procedures that include requesting, reviewing, approving, and documenting firewall rule changes. Procedures should also include the periodic review and recertification of the firewall rules.

Response

We agree with the recommendation. While firewall rule changes have been managed and authorized by the senior technical staff, we agree that more formal procedures should be in place. We have made good progress in establishing formal procedures. We will work with OET to address the recertification of the firewall rules of firewalls owned and operated by OET referenced in this finding.

Person responsible: Ron Olsen, Chief Security Officer and OET security personnel

Implementation date: June 2010

Recommendation

Finding 6. The Department of Management and Budget should define its password-related requirements, implement, and enforce strong password controls.

Response

We agree with the recommendation. As we discussed in our exit conference, this finding does not refer to the users of this system. The finding refers to several internally held system accounts managed by our technical staff. It is important to note that the audit did not uncover anything other than strong passwords in use in all accounts reviewed and all individuals were aware of the requirement for strong passwords to be used. Rather than software enforced strong passwords, our technical staff utilized system-generated strong passwords. Essentially the same result was accomplished. However, we agree we could use additional software features to enforce this and these software controls have been implemented. In addition, documentation of our password requirements will be implemented.

Person responsible: Ron Olsen, Chief Security Officer

Implementation date: April 2010

We appreciate the opportunity to participate in reviews such as this one by your organization and value your recommendations on how to further strengthen the strict controls we have implemented in the past to protect our data and systems.

Sincerely,

Tom J Hanson

Tom J. Hanson
Commissioner

THE OFFICE OF
ENTERPRISE**TECHNOLOGY**
STATE OF MINNESOTA

February 9, 2010

Mr. James Nobles, Legislative Auditor
Office of the Legislative Auditor
658 Cedar Street
Saint Paul, MN 55155

Dear Mr. Nobles:

I would like to thank you for the opportunity to respond to this audit of State Personnel and Payroll System Security Controls. OET concurs with the findings and recommendations in this report and will work with the Department of Minnesota Management and Budget to remedy the underlying issues.

Although the Department of Minnesota Management and Budget is the focus of this audit, it is important to note that individual agencies do not have the ability to address cyber security threats on their own – it requires a team effort of agency and OET staff. Combating complex cyber threats requires agency and OET specially-trained people, well-defined processes, and sophisticated tools that are simply beyond the reach of individual agencies. With our new Enterprise Security Program, OET has begun to put in place the people, process, and tools to provide consistent security controls across state government.

However, it is also important to note that the State of Minnesota's decentralized information technology environment is inherently difficult to secure. The over 36 executive branch data centers make it problematic to ensure that the necessary physical and technical security controls are provided.

Although the MMB IT infrastructure at issue in this audit is located in the OET data center, we continue to work on a data center consolidation strategy that will address the important and underlying issues that cause the state's broader security concerns. Our goal is to put in place the right people, process, and tools to provide consistent security controls enterprise wide. Stronger, more centralized management would enable all agencies to have better security controls. This is fundamental to reducing the state's risk and safeguarding our citizens' data.

In conclusion, I would like to thank you and your staff for the outstanding effort on this audit. I also look forward to working with policymakers and executive branch leaders to bridge our current security shortcomings.

Sincerely,

Gopal Khanna
Chief Information Officer
State of Minnesota