OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

Department of Management and Budget

Statewide Integrated Financial Tools (SWIFT)

July 2011 through July 2012

November 16, 2012 **Report 12-23**

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

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

November 16, 2012

Representative Michael Beard, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. James Schowalter, Commissioner
Department of Management and Budget

This report presents the results of our information technology and internal controls and compliance audit of the state's new accounting and procurement system – Statewide Integrated Financial Tools (SWIFT) for the period July 2011 through July 2012.

We discussed the results of the audit with the Department of Management and Budget's staff on October 30, 2012. We have included the department's response to our findings with this report. In addition, we have included the Department of Administration's response to Finding 3, which relates, in part, to its use of SWIFT.

The audit was conducted by Michael Hassing, CPA, CISA (Audit Manager), Scott Tjomsland, CPA, CISA (Audit Manager), Carolyn Engstrom, CISA, CISSP (Audit Manager) and assisted by many auditors from the Office of the Legislative Auditor.

We received the full cooperation of staff of the Department of Management and Budget and other state agencies 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

Report Summary

Conclusion

In developing and implementing the state's new accounting system, Statewide Integrated Financial Tools (SWIFT), the Department of Management and Budget designed internal controls that were generally adequate to ensure that the department:

- accurately processed and recorded financial transactions and data;
- protected not public data and limited unnecessary and incompatible access; and
- monitored and limited changes to SWIFT server security and databases to ensure changes were authorized.

However, some internal controls were not functioning as expected.

The Department of Management and Budget designed internal controls that were generally adequate to ensure compliance with applicable selected finance-related legal requirements. However, for the items tested, the department did not comply with some specific requirements.

The department resolved two of the four prior audit findings relevant to this audit. The two findings not resolved are included in this report.

Key Findings

- Prior Finding Not Resolved: The Department of Management and Budget did not sufficiently identify and communicate risks created by incompatible duties. (Finding 1, page 9)
- The Department of Management and Budget did not adequately restrict employees from processing payments to vendors who were not subject to the department's vendor validation process. (Finding 2, page 10)
- The departments of Management and Budget and Administration allowed employees who had SWIFT security access to create and maintain vendor data to make changes without adequate oversight and to have unmitigated incompatible access or unnecessary access. (Finding 3, page 11)
- The Department of Management and Budget did not implement internal controls to prevent or detect unauthorized access to not public data in the databases. (Finding 4, page 12)

Audit Objectives and Scope

To review the design of selected internal controls for the new accounting system the Department of Management and Budget placed in operation in July 2011.

Statewide Integrated Financial Tools (SWIFT) Review of Selected Internal Controls

Overview

On July 1, 2011, the Department of Management and Budget replaced the state's primary accounting system with a new system called the "Statewide Integrated Financial Tools" (SWIFT).[1] The system supports administrative functions across state agencies, including procurement, financial transaction processing, and internal and external financial reporting.

The state's various business processes and financial transactions flow through different components of SWIFT, referred to as "modules." The modules are designed to control and account for each type of financial activity and ensure the integrity of the resulting financial data. Table 1, on page 4, provides an overview of the SWIFT modules and their functions.

The Department of Management and Budget and the Office of Enterprise Technology[2] share management of the system's servers and databases, which comprise the system's technical infrastructure. The department managed SWIFT's development and implementation and now administers its overall account structure and business processes. The Office of Enterprise Technology provides various technical services, including system security, database management, batch operations monitoring, server administration, and vulnerability management.

After the initial implementation, the Department of Management and Budget has continued to enhance SWIFT's procurement process and the availability of financial reports and data. For the first part of fiscal year 2012, state agencies did not have fundamental budget and expenditures reports. In addition, the department continued to develop a data warehouse (now projected to be fully operational in April 2013).[3] As a temporary alternative, the department provided limited access to unformatted transaction data. Although it would have been preferable to have fully developed the system's reporting and data capabilities by the time the department put the system into operation, management felt that this deficiency was not a valid basis to delay the implementation for another year. By January 2012, although the

[1] To develop SWIFT, the State of Minnesota purchased and modified PeopleSoft Enterprise Resource Planning System, a proprietary product of Oracle, Inc. The state's existing human resources and payroll system is also an Oracle PeopleSoft system; the state integrated this existing system with SWIFT, and the two systems share some underlying infrastructure.

[2] *Minnesota Laws* 2011, First Special Session, Chapter 10, Article 4, consolidated the state's information technology services and personnel into the Office of Enterprise Technology, which recently changed its name to MN.IT Services.

[3] A data warehouse is a central repository of data used for reporting and data analysis. The data stored in a warehouse are first copied from production data (as raw data) into a "staging" database where it is arranged and organized into data warehouse tables that can be queried to create reports and extract data.

department had not completed its reporting and data warehouse development, state agencies had many financial reports, training materials, and reference guides available.

Table 1
Statewide Integrated Financial Tools (SWIFT)
Modules and Their Function

SWIFT Module	Function
Procurement Modules	
Vendor	Establishes vendor data, demographics, unique vendor identification numbers, and vendor bank account information.
eSupplier Connection	Provides information, in real time, to suppliers or vendors through an external facing application.
Supplier Contract Management	Allows users to create an electronic version of vendor contracts.
Strategic Sourcing	Allows users to select vendors from electronically submitted bids.
eProcurement	Allows users to create and manage requisitions, the first step in the purchasing process.
Purchasing	Allows users to create and process purchase orders.
Catalog Management	Maintains a list of items available from individual vendors.
Financial Modules	
General Ledger	Maintains the state's Chart of Accounts, creates accounting journals, and facilitates the fiscal year end close of financial activity.
Commitment Control	Establishes budget control through loading legally adopted appropriations, creating expense and revenue budgets, and allowing transfers between appropriations and budgets.
Accounts Payable	Allows users to process and manage vouchers and payments.
Grants Management	Enables state agencies to plan, manage, and track grants they receive from entities, such as federal agencies, local units of government, and nonprofit organizations.
Project Costing	Creates and monitors project budgets and costs.
Cost Allocations	Processes cost allocations and captures labor costs.
Accounts Receivable/Billing	Establishes accounts receivables, creates bills, manages receipts, and applies payments collected to receivable accounts.
Asset Management	Records, tracks, and depreciates state assets.
Inventory	Provides a comprehensive inventory management system.
Cash Management	Allows the user to reconcile the general ledger to the bank accounts and net interagency payments. (The state does not use this module's bank account reconciliation function.)

Source: Department of Management and Budget's SWIFT reference guides.

Objectives, Scope, and Methodology

This selected scope audit of SWIFT was our first examination of how SWIFT works. It was a high-level review of how the system processes and records the state's financial transactions. Our review of SWIFT will be ongoing as we examine how specific agencies process transactions through SWIFT and implement controls needed at the agency level.

The scope of this audit included applications related to system security, server and database management; interface applications; and the flow of financial activity through the business and workflow processes of various SWIFT modules.[4] We focused on the following audit objectives:

- Did the Department of Management and Budget design internal controls to ensure the integrity of recorded transactions and data, including those recorded through interfaces with other information systems; protect not public data; and limit unnecessary and incompatible system access?

- Did the Department of Management and Budget design internal controls to monitor and limit changes to SWIFT's server security and databases to ensure changes were authorized?

- Did the Department of Management and Budget design internal controls to ensure it complied with applicable legal requirements related to managing system data and financial transactions?

- Did the Department of Management and Budget resolve audit findings from prior audit reports that were relevant to this audit?[5]

To meet these audit objectives, we gained an understanding of the Department of Management and Budget's design of system controls and edits, financial policies, and procedures. We considered the risk of errors in the accounting records and potential noncompliance with relevant legal requirements. We analyzed accounting data for selected financial activity occurring through the various SWIFT modules during the initial implementation phase to identify system controls and edits and to ensure the accuracy and completeness of the financial

[4] Although the state's human resources and payroll system was not the primary focus of our audit, some of the conclusions we reached may be applicable to that system because it shares some servers and databases with SWIFT.

[5] Office of the Legislative Auditor, Financial Audit Division Report 11-24, *Department of Management and Budget, SWIFT Application Security Controls (Findings 2 and 3),* issued November 3, 2011; Office of the Legislative Auditor, Financial Audit Division Report 10-24, *Department of Management and Budget, Banking and Vendor Controls (Findings 2 and 4),* issued July 1, 2010.

data. We surveyed certain state agencies related to system security and certain system application controls.

Because the department had not fully developed SWIFT's reporting capabilities or its data warehouse, we limited our testing of the accuracy and availability of data to a verification that data in the SWIFT "staging" tables agreed with data and transactions recorded in SWIFT, and reviewed reports available as of June 2012 for a limited number of state agencies. This limited testing did not provide us with sufficient audit evidence to conclude whether state agencies had complete and accurate data available to monitor their financial activities. Also, as of June 2012, the Department of Management and Budget had not completed the design of its fiscal year end closing and financial reporting processes, and we did not include those processes in the scope of this audit.

We conducted the audit in accordance with generally accepted government auditing standards. 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 used various criteria to evaluate internal controls and compliance. We used, as our criteria to evaluate agency controls, the guidance contained in the *Internal Control-Integrated Framework*, published by the Committee of Sponsoring Organizations of the Treadway Commission.[6] To address security controls, we used criteria contained in the National Institute of Standards and Technology's *Special Publication 800-53 (Recommended Security Controls for Federal Information Systems).* We used state and federal laws, regulations, and contracts, as well as policies and procedures established by the Department of Management and Budget and other state agencies' internal policies and procedures as evaluation criteria over compliance.

Conclusion

In developing and implementing the state's new accounting system, Statewide Integrated Financial Tools (SWIFT), the Department of Management and Budget designed internal controls that were generally adequate to ensure that the department:

- accurately processed and recorded financial transactions and data;
- protected not public data and limited unnecessary and incompatible access; and

[6] The Treadway Commission and its Committee of Sponsoring Organizations were established in 1985 by the major national associations of accountants. One of their primary tasks was to identify the components of internal control that organizations should have in place to prevent inappropriate financial activity. The resulting *Internal Control-Integrated Framework* is the accepted accounting and auditing standard for internal control design and assessment.

- monitored and limited changes to SWIFT server security and databases to ensure changes were authorized.

However, some internal controls were not functioning as expected.

The Department of Management and Budget designed internal controls that were generally adequate to ensure compliance with applicable selected finance-related legal requirements. However, for the items tested, the department did not comply with some specific requirements.

The department resolved two of the four prior audit findings relevant to this audit. The two findings not resolved are included in this report.

The following *Findings and Recommendations* section provides further explanation about the exceptions noted above.

Findings and Recommendations

Finding 1

Prior Finding Not Resolved: The Department of Management and Budget did not sufficiently identify and communicate risks created by incompatible duties.[7]

The Department of Management and Budget did not complete a revised assessment of incompatible security roles to provide to state agencies' security liaisons. Without comprehensive and sufficient guidance about SWIFT security roles, security liaisons could not ensure that their agencies 1) avoided assigning incompatible security roles to employees, when possible, and 2) had effective internal controls in place to mitigate the risks created by the incompatible roles.

Security permissions are the building blocks of security roles; each permission grants the ability to perform something specific in SWIFT, such as performing an inquiry on a purchase order or recording an invoice. Certain combinations of permissions are deemed incompatible because they allow a single user to complete parts of a transaction that should be performed by multiple people to reduce the risk of error and fraud. For example, the permissions that provide the ability to approve a vendor should be separated from the permissions that provide the ability to enter or approve an invoice so that a person could not create a fictitious vendor and submit fictitious invoices.

Incompatible security roles result when multiple roles are assigned to a user and the combinations of permissions assigned to the roles create incompatibilities. The best solution is to identify combinations of roles that create incompatibilities and prevent them from being assigned to users. That is not always possible due to staff sizes and other factors. In those instances, other monitoring and review activities should be performed to reduce the risk of fraud or inaccuracies. However, effective mitigating controls cannot be implemented until the incompatibilities that pose a risk are clearly understood.

The department published documentation about incompatible roles in May 2011 based on the preliminary design of the security roles, but it did not update the guidance to reflect the access provided by the actual security roles. In February 2012, the department contracted with a consultant whose duties included, among other things, a comprehensive review of the security roles and permissions. The department plans to have updated security role descriptions and segregation of duties guidance available in December 2012, prior to the annual certification of security access due in January 2013. There are about 1,000 permissions that have been assigned to approximately 460 unique roles.

[7] Office of the Legislative Auditor's Financial Audit Division Report 11-24, *Department of Management and Budget, SWIFT Application Security Controls (Findings 2 and 3),* issued November 3, 2011.

The purpose of the incompatibility analysis is to provide accurate information to security liaisons so they understand the risks of assigning certain combinations of roles. Our survey of security liaisons produced some contradictory results. While a majority of those surveyed indicated that they agreed or strongly agreed with the statement, "I understand which combinations of roles create incompatibilities," they later responded that their biggest challenge as a security liaison was understanding incompatible duties and understanding the actual system access provided to employees through assigned roles and privileges.

Recommendation

- *The department should continue to review and revise security role descriptions; update and communicate segregation of duties documentation; and provide security liaisons resources and training to ensure they understand the security roles and privileges to perform their duties.*

Finding 2

The Department of Management and Budget did not adequately restrict employees from processing payments to vendors who were not subject to the department's vendor validation process.

About 250 employees in several state agencies had SWIFT security access that allowed them to make payments to vendors who had not been authorized through the Department of Management and Budget's vendor validation process. This access is high-risk because it may allow an employee to make an unauthorized payment without detection. The employees could type in any vendor name, address and bank account information to generate payments. We identified and reviewed the small number of payments made through this process from July 2011 through April 2012 and found these transactions were legitimate and authorized.

Although the SWIFT system allowed these types of payments, called "single payment vouchers," the Department of Management and Budget's staff told us they did not intend for state agencies to use them. The staff incorrectly believed only a few of their department's employees could perform this high-risk type of payment; they were unaware that employees in other agencies inadvertently had the access through the security roles their supervisors and security liaisons had approved. The department had not assessed the risks or developed policies or provided training about how or when to use the online single payment option and had not designed internal controls to detect any unauthorized transactions if they should occur.

Recommendation

- *The Department of Management and Budget should either restrict employees' SWIFT security access to process online single payment vouchers or develop internal controls to detect payments made to vendors not subjected to the department's vendor validation process.*

Finding 3

The departments of Management and Budget and Administration allowed employees who had SWIFT security access to create and maintain vendor data to make changes without adequate oversight and to have unmitigated incompatible access or unnecessary access.

The departments did not ensure the accuracy and integrity of the changes made by the 21 employees with the ability to create and approve new vendors and modify existing vendor data. All of these employees could change vendor addresses, and 12 could also change vendor bank account information without any secondary review or approval. The lack of a secondary review or approval increased the risk of erroneous or unauthorized changes to vendor data, which could allow an employee to redirect valid vendor payments to the employee's address or bank account.

In addition, the Department of Management and Budget did not implement mitigating controls for six of these employees who also had SWIFT security access to process payments to vendors, creating the ability to perform incompatible duties because the employee could establish a fictitious vendor and process payments to that vendor. The department did not establish internal controls to mitigate that risk, such as identifying and validating any payments these employees actually processed. State policy requires agencies to implement and maintain mitigating controls when they allow employees to have incompatible access.[8]

Finally, the Department of Management and Budget gave two of these employees SWIFT security access to functions that they did not need to perform their job duties. State policy requires agencies to limit employee access to only what is necessary for the employee to perform their job functions and responsibilities.[9]

The reviews and approvals of new vendors by employees of the departments of Management and Budget and Administration, and any subsequent changes they make to vendor data, are fundamental internal controls to ensure all state agencies make payments to legitimate vendors. Allowing these employees to make changes

[8] Department of Management and Budget Statewide Operating Policy 1101-07.

[9] *Ibid.*

without adequate oversight, to have unmitigated incompatible system access, or to have unnecessary access undermined this important internal control.

Recommendations

- *The departments of Management and Budget and Administration should establish oversight procedures to ensure the accuracy and integrity of vendor data changes made by their employees.*

- *The Department of Management and Budget should eliminate incompatible or unnecessary access for employees who create and approve new vendors and modify existing vendor data. If employees need incompatible access to perform their job duties, the department should establish effective internal controls to mitigate the risk of erroneous or fraudulent payments occurring without detection.*

Finding 4

The Department of Management and Budget did not implement internal controls to prevent or detect unauthorized access to not public data in the databases.

The Department of Management and Budget did not encrypt not public data fields, such as social security numbers and bank account information, within the databases to prevent incidental or unauthorized viewing. Lacking preventive controls to protect not public data, the department also did not implement the logging of users who accessed not public data fields to detect whether unauthorized access occurred.

State statutes require agencies to establish appropriate security safeguards for all records containing data on individuals.[10] Those safeguards would include ensuring that the data is not available to an unauthorized person, defined in statute as "any person who accesses government data without permission or without a work assignment that reasonably requires the person to have access to the data."[11]

By not encrypting the data or logging access to the data, the department increased the risk that not public data could be inappropriately accessed without detection. Three database administrators and about 70 users with access to databases can view or extract not public data in clear text. Department staff did not encrypt the not public data because they thought it would negatively affect the performance of the databases. While database performance is a valid operational criterion to consider before implementing encryption, the department had not performed

[10] *Minnesota Statutes* 2011, 13.05, subd. 5.

[11] *Minnesota Statutes* 2011, 13.055, subd. 1, paragraph d.

testing to determine what impact, if any, encryption actually had on database performance.

In the absence of adequate preventive controls, logging those who viewed the data and monitoring the logs would detect if a user had inappropriately viewed not public information. However, the department did enable logging to detect any changes to data within the databases. Securing database level access is important because it operates independently from the security roles that limit the screens and fields a user is able to view and execute within the SWIFT application.

Recommendations

- *The department should log and review access to database tables that contain not public data.*
- *The department should test encryption to determine the impact on database performance.*

Finding 5

Prior Finding Not Resolved: The Department of Management and Budget authorized four employees to have unnecessary access to the state's bank accounts.[12]

The department granted four employees the ability to make electronic payments from state bank accounts; this access was not necessary for the employees to perform their job duties. The unnecessary access would allow the employees to make electronic payments without the involvement or authorization of another employee. Although the department eliminated the unnecessary access identified in our 2010 audit report, it did not put internal controls in place, such as a periodic review of employee bank account access, to prevent it from recurring.

State policy requires agencies to limit access to only those functions an employee needs to perform job duties.[13] The risk of errors and fraud increases when employees have unnecessary access.

Recommendation

- *The department should eliminate unnecessary access to the state's banking applications and periodically review employees' access to the bank accounts.*

[12] Office of the Legislative Auditor, Financial Division Report 10-24, *Department of Management and Budget, Banking and Vendor Controls (Finding 4),* issued July 1, 2010.

[13] Department of Management and Budget Policy 1101-07.

Finding 6

The Department of Management and Budget had not implemented adequate logging of significant operating system events.

The department did not log certain system events, such as adding new users or changes to security policy, to protect the integrity of the system's configuration. Although the department had implemented logging of standard events and of users accessing payment files, enabling logging of other types of events would provide information about changes made to the operating system and files that the operating system protects. SWIFT is integral to the state's financial operations; the department categorized the servers supporting the SWIFT application as high impact. High impact systems generally require more logging than less important systems because of the nature of the data they contain. By ensuring additional system events are reviewed, the department can determine whether the changes were authorized and complied with change management procedures, or if the change was due to a system hack or malicious attack.

Recommendation

- *The department should evaluate the logging of system events and modify review procedures to ensure compliance and detection of unauthorized changes.*

Finding 7

The Department of Management and Budget did not implement sufficient controls to monitor compliance with its system security practices.

The department did not have adequate controls to detect deviations from its stated security practices. The department had the following areas of noncompliance:

- Administrators assigned some security privileges directly to users in the operating system and database rather than assigning the privileges to groups. This security practice was not documented in the security plans, but had been verbally communicated to the administrators.

- Database administrators had not enabled password complexity as indicated in the database security plan on one database profile, which resulted in 36 users not subject to password complexity.

- Server administrators did not set the minimum password length to the length dictated by department policy for privileged accounts. Although the department directed users to have passwords that complied with the policy, the system would not reject noncompliant passwords.

- For one nonadministrative account, database administrators had not changed the password from the manufacturer's default password and had

not disabled the account. For four other accounts, the department also had not changed the password from the manufacturer's default password, but had locked the accounts.

Although the instances of noncompliance we detected did not pose significant risks to the system's overall security, management was not aware of and had not authorized these deviations from its policies and standards. By enhancing monitoring procedures to periodically evaluate whether system configurations and settings comply with policies and standards, the department can ensure that security practices have been implemented as intended.

Recommendation

- *The department should periodically monitor whether system configurations and settings comply with the department's security practices.*

SWIFT did not accurately calculate depreciation for some long-term capital assets.

Finding 8

SWIFT did not accurately calculate depreciation for capital assets with useful lives that extended beyond June 30, 2040, the calculation's default end date. As a result, the system calculated depreciation for those assets through the default end date rather than through the asset's entire useful life. Left uncorrected, this error would have resulted in an overstatement of the current year's depreciation expense and an understatement of the year end asset balance. Although the errors were quite small for fiscal year 2012, if the calculation is not corrected, the errors will become larger as more assets' useful lives extend beyond the default date and the errors accumulate over time.

Recommendation

- *The department should correct the capital asset depreciation calculation to ensure the accuracy of the depreciation calculation and the year end capital asset balance.*

MINNESOTA Management & Budget

November 9, 2012

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

RE: SWIFT Information Technology Audit

Dear Mr. Nobles:

Thank you for the opportunity to discuss your findings on the recent SWIFT audit. We are committed to strong financial controls, and we value suggestions to make our processes even stronger. Strong controls were an important part of our system design, and we have worked hard to implement an accurate and secure system. As you know, information system implementations of this size and complexity are challenging, and we are pleased that you found that we designed controls that are generally adequate. We have addressed each of your recommendations below.

Recommendation – Finding 1

The department should continue to review and revise security role descriptions; update and communicate segregation of duties documentation; and provide security liaisons resources and training to ensure they understand the security roles and privileges to perform their duties.

Response:

We have completed our work to review and update security roles and permissions, and we are in the final phase of documenting and testing the changes. Updated documentation and training will be provided to agencies including segregation of duties guidance and materials on mitigating controls. We expect to complete our annual recertification of security access in January 2013.

Person responsible: Lori Mo, Assistant Commissioner, Accounting Services
Estimated completion date: January 2013

Recommendation – Finding 2

The Department of Management and Budget should either restrict employees' SWIFT security access to process online single payment vouchers or develop internal controls to detect payments made to vendors not subjected to the department's vendor validation process.

Response:

Our intention for this security role was to allow resolution of batch interface errors only. When you identified the broader authority, we acted to remove SWIFT security access to process on-line single payment vouchers. A new process is in place to prevent giving this role to new users.

Person responsible: Ron Mavetz, Agency Support Director
Completed

Recommendation – Finding 3

The departments of Management and Budget and Administration should establish oversight procedures to ensure the accuracy and integrity of vendor data changes made by their employees.

The Department of Management and Budget should eliminate incompatible or unnecessary access for employees who create and approve new vendors and modify existing vendor data. If employees need incompatible access to perform their job duties, the department should establish effective internal controls to mitigate the risk of erroneous or fraudulent payments occurring without detection.

Response:

We will review work assignments and, whenever possible, we will limit employee authority to modify vendors, or make payments, but not both. When this is not possible, we will design and implement mitigating controls. We will modify our business process to add a secondary review to the vendor change process to provide oversight for changes to highly sensitive items such as bank accounts.

Person responsible: Ron Mavetz, Agency Support Director
Estimated completion date: December 2012

Recommendation – Finding 4

The department should log and review access to database tables that contain not public data.
The department should test encryption to determine the impact on database performance.

Response:

We agree that encryption adds another level of protection and that it does come at some cost. We will evaluate the impact of encryption on system performance and expect that we would be able to implement encryption on fields with high sensitivity. In combination with these changes, we will evaluate whether additional logging and monitoring of certain activities is warranted.

Persons responsible: John Vanderwerf, MN.IT @ MMB Chief Technology Officer, working with MN.IT central
Implementation date: April 2013

Recommendation – Finding 5

The department should eliminate unnecessary access to the state's banking applications and periodically review employees' access to the bank accounts.

Response:

We have reviewed our existing controls on banking application access. We have identified and implemented changes to strengthen our review process prior to granting access, and we have formalized our review and documentation practices.

Person responsible: Michi Eichinger
Completed

Recommendation – Finding 6

The department should evaluate the logging of system events and modify review procedures to ensure compliance and detection of unauthorized changes.

Response:

We agree that we should review the events that are being logged and those that could be added to the logging and reporting process. We will evaluate and make changes based on this review.

Persons responsible: John Vanderwerf, MN.IT @ MMB Chief Technology Officer, working with MN.IT central

Implementation date: February 2013

Recommendation – Finding 7

The department should periodically monitor whether system configurations and settings comply with the department's security practices.

Response:

We agree with the recommendation. As noted in the report and the exit conference, the department's security practices require strong controls. We agree it would be good practice to periodically confirm that there are no deviations from the strong control practices we require. We will incorporate additional review for these controls in our annual security certification process.

Persons responsible: John Vanderwerf, MN.IT @ MMB Chief Technology Officer
Implementation date: February 2013

Recommendation – Finding 8

The department should correct the capital asset depreciation calculation to ensure the accuracy of the depreciation calculation and the year-end capital asset balance.

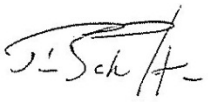
Response:

Our initial system configuration limited some building depreciation calculations to an incorrect useful life. The problem was discovered and corrected prior to year-end depreciation calculations.

Person responsible: Ron Mavetz, Agency Support Director
Completed

Thank you for your recommendations. We value your audit work and the improvements it generates further improve our financial management practices.

James Schowalter



Commissioner
Minnesota Management & Budget

November 9, 2012

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

Dear Mr. Nobles:

Thank you for the opportunity to review the results of the information technology and internal controls and compliance audit related to the State of Minnesota's new accounting and procurement system – Statewide Integrated Financial Tools (SWIFT). On behalf of the Department of Administration (Admin), I wish to extend my appreciation to you and your staff for the work done to help assure secure and effective implementation of the new system.

The audit contained one finding for Admin, relating to security of vendor data:

Finding 3
The departments of Management and Budget and Administration allowed employees who had SWIFT security access to create and maintain vendor data to make changes without adequate oversight and to have unmitigated incompatible access or unnecessary access.

Recommendation
The departments of Management and Budget and Administration should establish oversight procedures to ensure the accuracy and integrity of vendor data changes made by their employees.

The audit found that 21 state employees could change vendor addresses without any secondary review or approval. Four of the 21 employees work in Admin's Materials Management Division (MMD). Admin appreciates the identification of this risk and is taking steps to eliminate the risk.

With the transition from MAPS to SWIFT, the vendor workflow process has changed significantly and MMD's duties related to this change have been reduced. The sole remaining task that adds genuine value is MMD's maintenance of "targeted group/economically disadvantaged" (TG/ED) small business certification status.

Admin is working to eliminate the security risk by limiting MMD's authorized role to the management of the TG/ED certification status. That will reduce the number of authorized individuals from four to two (regular and backup). Limiting MMD's role to modifying TG/ED status will eliminate the risk of changed

addresses. Additionally, the TG/ED status changes will trigger workflow back to Minnesota Management and Budget for independent review and approval.

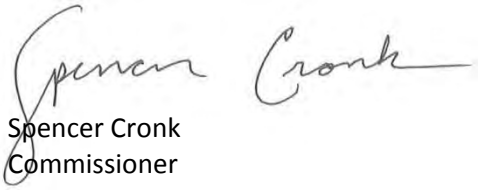
Removing MMD's authority to make other changes, such as vendor addresses, will require a modification to the system. Admin will work with Management and Budget, the SWIFT steering committee and project staff and will attempt to implement this change. In the interim, we will explore the feasibility of routing the relatively small number of vendor changes made during the approval process back to MMB for review.

Person responsible:
Kent Allin, Director, Materials Management Division (651) 201-2400

Target date for resolution of the audit issue:
Admin does not have direct control of the individuals and the other resources needed to modify the system. Admin staff members will work with colleagues in Management and Budget and attempt to make the change as soon as is practicable.

Thank you again for your thoughtful analysis of SWIFT security risks and calling this matter to our attention.

Sincerely,



Spencer Cronk
Commissioner