OLA
OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

FINANCIAL AUDIT DIVISION REPORT

# Department of Management and Budget

## Banking and Vendor Controls

## Internal Control and Compliance Audit

**July 1, 2010** **Report 10-24**

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. Tom J. Hanson, Commissioner
Department of Management and Budget

This report presents the results of our audit of the Department of Management and Budget's banking and vendor controls. This was an internal control and compliance audit of disbursements from the state treasury and specifically addressed the department's controls over the electronic payments made through the state's accounting and payroll systems, the warrants issued from these two systems, and the vendor files maintained in the accounting system. We emphasize that this has not been a comprehensive audit of the Department of Management and Budget.

We discussed the results of the audit with the department at an exit conference on June 22, 2010. This audit was conducted by Michael Hassing, CPA, CISA (Audit Manager) and Laura Wilson, CPA, CISA (Auditor-in-Charge), assisted by auditors Bill Betthauser, CISA, Melanie Greufe, Pat Ryan, and Adam Spooner.

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

We received the full cooperation of the department 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

The Department of Management and Budget's internal controls over banking disbursements and vendor arrangements were generally adequate to ensure that the department prevented unauthorized payments from the state's bank accounts, safeguarded state warrants, accurately paid the state's vendors, protected not public vendor data (including bank account information), and acted in accordance with management's authorization.

For the items tested, the Department of Management and Budget generally complied with the significant legal-related requirements.

However, the department did not adequately manage the vendor files within the state's accounting system and had other control weaknesses. The following *Findings and Recommendations* provide further explanation about these control weaknesses.

## Findings

- The department did not adequately assess its business risks or monitor the effectiveness of its internal controls over the state's disbursements and vendor files in the state's accounting system. (Finding 1, page 7)
- The department did not adequately manage the vendor files within the state's accounting system. (Finding 2, page 8)
- The department did not sufficiently restrict access to some data files containing not public vendor information. (Finding 3, page 10)
- The department allowed incompatible access to the state's accounting system and unnecessary access to the bank's web-based application. (Finding 4, page 11)
- The department did not adequately control some payments made outside the state's regular payment process. (Finding 5, page 12)

## Audit Objectives and Scope

| Objectives | Period Audited |
|---|---|
| • Internal Control and Legal Compliance | Fiscal Year 2010 |

Areas Audited

We audited the department's controls, including the state treasury's controls, over the electronic payments made through the state's accounting and payroll systems, the warrants issued from these two systems, and the vendor files maintained in the accounting system.

# Department of Management and Budget

## Overview

The Department of Management and Budget operates under *Minnesota Statutes* 2009, Chapter 16A. These statutes direct the department to manage the state's financial affairs by receiving and recording all money paid into the state treasury and safely keeping it until lawfully paid out.[1] To facilitate these responsibilities, the department manages the state's accounting and payroll systems. Through these systems, employees initiate payments to vendors and employees. More than one hundred state subsystems interface with the state's accounting and payroll systems.

The State of Minnesota disburses more than $30 billion each fiscal year from the state treasury. It makes 85 percent of these disbursements through electronic fund transfers. Electronic fund transfers (EFT) are the exchange or transfer of money electronically from one account to another, either within the same bank or between different banks. There are two types of EFT transactions:

- A **wire transfer** moves money from the state treasury to a specific bank account. The state uses repeat transfers to move funds frequently to the same recipients. The treasury establishes a standard template for these repeat transfers, and the bank requires only one approval before moving the funds. The remaining wire transfers are one-time transfers and require two approvals.

- An **Automatic Clearing House (ACH)** transaction moves money between the treasury account and multiple vendor or employee bank accounts. When processing ACH payments, either the department or another state agency electronically transmits the detailed payment data to the bank. The bank holds the information until it receives final approval from the state's treasury staff, then the bank forwards the data to the clearing house. The clearing house moves the money into the payees' bank accounts.

The State of Minnesota uses paper state warrants to make the remaining 15 percent of payments to vendors and employees.[2] The Department of Management and Budget has an agreement with the Department of Employment and Economic

[1] *Minnesota Statutes* 2009, 16A.055, Subd. 1. In 2003, because of a change to the state constitution abolishing the Office of the State Treasurer, the department incorporated state treasury operations into its other duties.

[2] A state warrant is similar to a check, with the state treasury acting as the bank.

Development to print and mail the state warrants.[3] Once the payees deposit the warrants, the local banks remit the warrants to either US Bank or Wells Fargo Bank which, in turn, remit the warrants to the state treasury for payment.

The Department of Management and Budget also maintains vendor information in the state's accounting system. Generally, state agencies request, through the accounting system, the set up of new vendors or changes to some vendor information. The department's system compliance/file maintenance unit then electronically approves the new vendor or change. However, the department works directly with the vendors to obtain or change vendor banking data needed to make ACH payments.[4]

The department relies on the Office of Enterprise Technology's technical resources to manage the state's mainframe, which houses the state's accounting systems.

# Objectives, Scope, and Methodology

We focused our audit on disbursements from the state treasury and specifically assessed the department's controls over the electronic payments made through the state's accounting and payroll systems, the warrants issued from these two systems, and the vendor files maintained in the accounting system.

Our objectives were to answer the following questions related to fiscal year 2010:

- Did the Department of Management and Budget have adequate internal controls to ensure that it prevented unauthorized payments from the state's bank accounts, safeguarded state warrants, maintained accurate vendor files in the state's accounting system, accurately paid the state's vendors, protected not public vendor and employee data, including bank account information, and acted in accordance with management's authorization?

- Did the Department of Management and Budget comply with applicable legal requirements, including *Minnesota Statutes*, and state and department policies?

To meet the audit objectives, we gained an understanding of the state's financial policies, processes, and procedures for disbursing state funds by discussing the significant responsibilities of employees and key processes of the departments of Management and Budget, Employment and Economic Development, Administration, and the Office of Enterprise Technology. We considered the risk of errors in the accounting records and potential noncompliance with relevant legal requirements. We analyzed vendor and disbursement data to identify

[3] These warrants are primarily for payment data generated from the state's main accounting and payroll systems.
[4] Banking data includes the bank routing and account numbers.

unusual trends or significant changes in financial operations. On a sample basis, we examined financial transactions and reviewed supporting documentation to test whether the department's controls were effective and if the transactions complied with laws, regulations, policies, and contract provisions. We used a variety of computer-assisted auditing tools and other techniques to analyze the security infrastructure and test information technology controls.

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 control and compliance. We used, as our criteria to evaluate the department's controls, the guidance contained in the *Internal Control-Integrated Framework*, published by the Committee of Sponsoring Organizations of the Treadway Commission.[5] To assess security controls, we used criteria published by the National Institute of Standards and Technology's Computer Security Division. We used state laws, regulations, and contracts, as well as state policies and procedures established by the department and the department's internal procedures as evaluation criteria over compliance.

# Conclusion

The Department of Management and Budget's internal controls over banking disbursements and vendor arrangements were generally adequate to ensure that the department prevented unauthorized payments from the state's bank accounts, safeguarded state warrants, accurately paid the state's vendors, protected not public vendor and employee data, including bank account information, and acted in accordance with management's authorization.

For the items tested, the Department of Management and Budget generally complied with the significant legal-related requirements.

However, the department did not adequately manage the vendor files within the state's accounting system and had other control weaknesses. The following *Findings and Recommendations* provide further explanation about these control weaknesses.

[5] 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.

# Findings and Recommendations

## Finding 1

**The Department of Management and Budget did not adequately assess its business risks or monitor the effectiveness of its internal controls over the state's disbursements and vendor files in the state's accounting system.**

The department had not comprehensively assessed its risks related to paying vendors and employees along with maintaining sensitive information in vendor files within the state's accounting system. These risks relate to protecting the state's bank accounts from unauthorized disbursements, accurately recording financial activity, and complying with finance-related legal requirements. While the department had many documented procedures, it did not assess whether these procedures were effective to prevent or detect errors and fraud. In addition, the department did not have a comprehensive plan to monitor the effectiveness of its internal controls over these critical functions. A comprehensive internal control structure is critical for safeguarding resources and financial information in the state's complex environment. Findings 2 through 5 identify significant weaknesses in the department's internal controls.

Had the department developed and implemented procedures to assess risks and monitor the effectiveness of its controls over critical banking functions and vendor payment processes, it could have identified and corrected the significant weaknesses identified in Findings 2 through 5, and addressed the following situations we observed:

- On April 20, 2010, we noted almost 700 returned warrants totaling over $206,000 unattended at an employee's desk. The department informed us that it only locked the warrants at the end of the business day.

- The department had not put stop payments on 6 of 142 original fiscal year 2010 warrants we tested when it issued replacements for warrants that had been lost or damaged. Without a stop payment, the department could inadvertently clear the original warrant rather than the replacement warrant.

- The department's contract with US Bank did not require that the bank provide written assurances or independent assessments about its security controls over information systems used for processing the state's financial transactions or its protection of not public data.

- The department's treasury division did not have written policies and procedures that addressed its cash management or banking practices. This

documentation would be critical for emergency operations or succession planning.

- The Department of Employment and Economic Development did not use passwords to restrict access to the computer used to print state warrants. Although the computer was in a secured room, over 50 people had key card access to the computer room, including nonstate employees maintaining the rented office space.

The state's policy on internal controls requires that each agency head identify, analyze, and manage business risks that impact the entity's ability to maintain its financial strength and the overall quality of its products and government services.[6] The policy further requires follow-up procedures that, at a minimum, should include ways to monitor controls and report significant weaknesses to individuals responsible for the process or activity involved, including executive management and those individuals in a position to take corrective action.

*Recommendation*

- *The department should develop and implement procedures to ensure it identifies financial risks and monitors the effectiveness of its internal controls for its critical banking functions and vendor payment processes.*

## Finding 2

**The Department of Management and Budget did not adequately manage vendor files within the state's accounting system.**

The department did not verify the legitimacy of new vendors added to the state's accounting system or changes made to current vendor information, including addresses, phone numbers, and contact names. In addition, the department did not guard against keying errors when entering vendor bank routing and account numbers and did not promptly purge obsolete vendors.

While the department performed some limited procedures, it generally authorized state agencies' requests to establish new vendors or make changes to vendor information without validating important vendor data, such as its tax identification number, address, contact person, or phone number. Department staff asserted that they did not have sufficient resources to validate the hundreds of vendor changes requested each day. However, the department had not fully assessed how it could automate, monitor, or verify, on a sample basis, the validity of this important data. We discussed several additional tests and validation processes the department could consider to enhance its review of vendor information.

[6] Department of Management and Budget Policy 0102-01 *Internal Control.*

The lack of verification of vendor data and data changes increases the risk that the state could process a payment to the wrong vendor or a fictitious vendor. Through the course of our audit, we identified nine questionable vendors receiving state payments, which we referred to the department for further investigation. The department provided plausible explanations for six of these vendors, and as of June 2010, continued to research and investigate the remaining three vendors. Vendor payments to those three accounts from July 1, 2007, through March 23, 2010, totaled $188,058.

Although the department required vendors to submit written EFT request forms when establishing payments via EFT or making changes to certain information, it did not require vendors to document their authorizations for all changes. In addition to changes submitted by state agencies, vendors also contacted the department directly to request changes to their vendor data. The department did not have adequate controls to ensure that all changes were authorized and validated. Changes in vendor information present risks for the state in making accurate and valid payments.

In addition, the department did not have controls to prevent or detect keying errors when entering vendor's banking information into the state's accounting system. The department relied on the bank's validation of the account as its primary control to identify inaccurately input accounts. For example, the department had incorrectly input one of the 29 EFT request forms we tested, but the bank rejected the change because the bank account number was not valid. However, in September 2009, the department incorrectly input another bank account number that was not the vendor's account but was a valid account at the bank; the state subsequently processed payments totaling nearly $30,000 to the wrong account. The error was not discovered until the intended vendor notified the department that it had not received payment.

Finally, the department did not purge obsolete vendors in accordance with its internal procedures.[7] Those procedures require the department to purge vendors that do not have any activity within two years or are designated as one-time-payment vendors, more than 30 days old. As of April 2010, the state's accounting system had over 133,000 active vendors (17 percent of total vendors) that met the criteria to be purged. The department explained that it had not purged vendors because, after the collapse of I-35W bridge in August 2007, the Attorney General's Office had prohibited the department from deleting, overwriting, or otherwise destroying or altering electronic information "relating to the I-35W bridge or any other bridge." We think the department's decision to suspend its automatic purging of inactive vendors was too broad of an interpretation of this directive. Purging inactive vendors is an effective internal control to reduce the risk of inappropriate or fraudulent transactions.

[7] Department of Management and Budget internal procedure "Vendor Purge."

By not maintaining accurate vendor files, the department increased the risk that a state employee with incompatible access to the state's accounting system could process fraudulent payments without detection. As of March 2010, more than 200 employees had incompatible access to the state's accounting system.[8]

*Recommendation*

- *The department should develop control and monitoring procedures to ensure that vendor information and subsequent changes to that information are valid, accurate, authorized, and current.*

## Finding 3

**The Department of Management and Budget did not sufficiently restrict access to some data files containing not public vendor information.**

The department did not have adequate controls to limit access to data files containing not public vendor and banking information. The department had not monitored or reviewed who had access to these sensitive files. Nearly 200 people and administrative software program accounts from the departments of Management and Budget, Transportation, and Office of Enterprise Technology had unnecessary access to read data files containing not public bank account information used for ACH and warrant payments. In addition, 70 Office of Enterprise Technology staff and administrative software program accounts had unnecessary access to modify these files. While the sensitive ACH files from the state's accounting system were temporarily stored on the Department of Management and Budget's computers and internal network, 13 people had unnecessary modify access.

The ability to read and modify sensitive files used in banking and other processes should be limited to only those people and administrative software program accounts needing that access.[9] By allowing excessive access, the department increased the risk that someone could inappropriately see, use, sell, or change the not public information.

Finally, the department had not assessed its need to monitor unauthorized access to files containing not public data. It had not customized its computers to log key security events. Monitoring is important in detecting and promptly responding to security events to ensure unauthorized individuals have not read or modified the files or data.[10]

[8] Employees could request vendor information, encumber funds, and make disbursements.
[9] National Institute of Standards and Technology 800-53, AC-6 *Least Privilege.*
[10] National Institute of Standards and Technology 800-53, AU-2 *Auditable Events,* AU-3 *Content of Audit Records,* and AU-6 *Audit Review, Analysis and Reporting.*

*Recommendations*

- *The department should further restrict employee access to files containing not public data and periodically review the access to ensure it is still needed.*

- *The department should develop a monitoring process to assess unauthorized access to files containing not public data.*

## Finding 4

**The Department of Management and Budget allowed incompatible access to the state's accounting system and unnecessary access to the bank's web-based application.**

The department gave five department employees incompatible access to the state's accounting system. These five employees had the ability to cancel electronic payments, reissue those payments via warrants, and update the vendor files. These functions represent unique responsibilities required to be performed only at the department, but not by the same person. The department defined incompatible access for receipt and disbursement functions performed by other state agencies but did not define or monitor incompatible access for its own employees and processes with these unique responsibilities.

The department did not detect or correct inappropriate access the bank provided to five employees of other state agencies. The accesses allowed the employees to perform disbursement transactions from three different state bank accounts. The bank inadvertently established the access when it migrated to a new application. The department did not, however, sufficiently monitor or question this access. We verified that no inappropriate disbursements were made from the three accounts.

State policy requires agencies to limit access to only those functions an employee needs to perform job duties and to avoid allowing incompatible access to accounting systems.[11] The risk of errors and fraud increases when employees have incompatible or excessive access to the state's accounting system and banking applications. Had the department reviewed employees' access, it could have identified and corrected the incompatible and excessive access.

*Recommendations*

- *The department should eliminate incompatible and unnecessary access to the state's accounting system and banking applications.*

[11] Department of Management and Budget Policy 1101-07 *Security and Access.*

- *The department should identify incompatible security groups that its employees have to perform the department's unique responsibilities.*

- *The department should periodically review employee access to ensure the roles granted are necessary and compatible with their current job functions.*

## Finding 5

**The Department of Management and Budget did not adequately control some payments made outside the state's regular payment process.**

The department did not adequately control some payments made through the warrant special handling process, also referred to as the pull warrant process. The warrant special handling process allows a printed state warrant to be "pulled" from the mail and brought to the department for additional procedures, rather than the usual process of mailing the warrant directly to the payee. The allowable types of pull warrants are: 1) warrants pulled to support wire transfers, 2) warrants pulled to attach special enclosures and then mailed,[12] and 3) warrants pulled for agencies to pick up at the department. Pull warrants increase the risk of unauthorized payments because they bypass the controls established in the normal payment process. Pull warrants allow possible inappropriate access to the warrants rather than ensuring that the state mails the warrants directly to the vendors.

The department had the following weaknesses in its pull warrant process:

- The state policy related to pull warrants did not adequately address significant risks in the warrant special handling process.[13] The policy did not specify the requirements for agencies picking up pull warrants and did not adequately address the risks related to pull warrants for wire transfers.

  - The department's instructions to agencies for the pull warrant process did not designate who should have the authority to authorize a pull warrant and did not prohibit someone authorizing or processing the transaction from picking up the warrant.[14] These duties are incompatible because, under some circumstances, they would allow someone to execute a payment and pick up the warrant, inappropriately increasing the risk of fraudulent payments. As of April 2010, approximately 180 state employees

[12] The Department of Management and Budget encloses the documentation and mails the warrants.

[13] Department of Management and Budget, Policy 0803-02 *Warrant Special Handling Request.*

[14] In February 2009, the department issued a memo to all state agencies requiring additional authorization and documentation for pull warrants.

could both authorize the warrant special handling forms and pick up the warrants.

- The warrant special handling request form only required one agency signature to authorize pull warrants for wire transfers (not for pick up by the agency). The department required agencies to process a pull warrant to support wire transfers to ensure proper recording of the disbursement in the state's accounting system. The person submitting the special warrant handling form also gave the department the banking information for the wire transfer. The department did not require a second authorization and did not have a list of employees authorized to request the wire transfers. By not requiring adequate authorization, the state risked fraudulent wire transfers.

- For 3 of 59 items we tested in fiscal year 2010, the department allowed an unauthorized person to pick up warrants or did not require the person picking up a warrant to sign the register. Both actions were inconsistent with directives the Department of Management and Budget had provided state agencies. Beginning in February 2009, the department required agencies to submit lists of employees authorized to pick up warrants and required employees picking up the warrants to show identification and sign a register.

- The department allowed staff from the Department of Employment and Economic Development, the department that printed the warrants, to obtain pull warrants directly from the warrant printing office. While this was convenient for the staff involved, it bypassed the Department of Management and Budget's controls designed to ensure that only authorized employees had access to warrants.

*Recommendations*

- *The department should enhance the state's warrant special handling policy to address the risks related to obtaining pull warrants and wire transfer transactions.*

- *The department should obtain appropriate and adequate authorization from state agencies before it allows warrants to be picked up or processes wire transfer transactions.*

MINNESOTA Management & Budget

June 28, 2010

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

RE: Banking Disbursements & Vendor Control Audit

Dear Mr. Nobles:

Thank you for the opportunity to discuss your findings on the Banking and Vendor Control audit. We are committed to strong financial controls and we value suggestions which will make our existing processes even stronger. In a number of areas you have identified, process improvements have already been made. Other changes are in progress, and additional improvements will be in place next year when our new accounting system (SWIFT) becomes operational.

**Recommendation – Finding 1**

The department should develop and implement procedures to ensure it identifies financial risks and monitors the effectiveness of its internal controls for its critical banking functions and vendor payment processes.

**Response**

While Minnesota Management & Budget (MMB) has numerous internal controls in place and makes regular management level risk assessment decisions about where to focus and apply mitigation strategies, we agree that we can do more to identify, monitor, and document controls. In some areas additional documentation is needed. We will work with the agency's Internal Control unit to enhance our risk management framework. Because of the on-going changes in programs, in technology and security threats, this will be an on-going effort.

These steps will be part of this effort:

- Continue to refine our risk assessment methodology
- Develop and update the necessary written policies, standards, and procedures
- Perform regular risk assessments
- Develop and implement changes as a result of the risk assessment decisions

To address the specific situations you identified, we have changes planned for the returned warrant handling process. Our existing process calls for a stop payment on all lost warrants prior to re-issue; the failures cited will be addressed as a training issue.

400 Centennial Building • 658 Cedar Street • St. Paul, Minnesota 55155
Voice: (651) 201-8000 • Fax: (651) 296-8685 • TTY: 1-800-627-3529
An Equal Opportunity Employer

The department's contract with US Bank did not require the bank provide written assurances or independent assessments about its security controls over information systems. Currently, the treasury division does not take an independent assessment of US Bank's internal controls. However, the bank is audited both internally and externally, and is regulated by a wide range of entities, including the Federal Office of the Comptroller of Currency (OCC). The plan to address this recommendation is for the Director of Treasury Operations to meet with our relationship manager at US Bank to address any findings from these independent assessments.

The treasury division currently does not have written policies and procedures outside of our continuity of operations plan. However, treasury staff have direct knowledge of all policies and procedures due to verbal communication, and there is little turnover in the division. A three month plan for writing these oral policies and procedures will be created.

Person responsible: Deloris Staffanson, Agency Support Director and
Joe Howe, Treasury Operations Director

Implementation date: October 2010 for specific observations, ongoing work on risk assessment.

**Recommendation – Finding 2**

The department should develop control and monitoring procedures to ensure that vendor information and subsequent changes to that information are valid, accurate, authorized, and current.

**Response**

With the size and complexity of the state's operations, and with approximately 150 new vendors added daily to the accounting system, we have historically relied on agency requests for vendor additions. For changes to existing vendors, we have already strengthened our controls for certain high risk changes. Further controls will be implemented with the new accounting system (SWIFT). When SWIFT is implemented July 2011, vendor information will be entered through a secure self service portal. On-line completion of W-9 information will be required before approval for most vendors. A weekly process has been implemented to verify banking account and routing number changes. A similar duplicate entry system has been designed for the new accounting system. When we have completed research on the remaining vendors identified, we will evaluate the risk and design ongoing controls.

Our regularly scheduled process to purge obsolete vendors was interrupted due to a litigation hold related to the I-35W bridge collapse in August 2007. The instructions for data retention received from the Attorney General's Office were comprehensive; we believe delaying the purge process was the proper response. MMB has recently obtained approval from the Attorney General's Office to purge old data after a backup file has been made and plans to do so are underway.

Person responsible: Deloris Staffanson, Agency Support Director

Implementation date: July 2011

**Recommendation – Finding 3**

The department should further restrict employee access to files containing not public data and periodically review the access to ensure it is still needed.

The department should develop a monitoring process to assess unauthorized access to files containing not public data.

**Response**

These recommendations have been and continue to be in place for our agency 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: Deloris Staffanson, Agency Support Director and
John Vanderwerf, Chief Technology Officer, working with OET management

Implementation date: October 2010

**Recommendation – Finding 4**

The department should eliminate incompatible and unnecessary access to the state's accounting system and banking applications.

The department should identify incompatible security groups that its employees have to perform the department's unique responsibilities.

The department should periodically review employee access to ensure the roles granted are necessary and compatible with their current job functions.

**Response**

The security access for the five MMB employees has been reviewed and access for two of them will be reduced to remove the incompatible functions. For the remaining three employees, access to vendor files will be reviewed to determine whether additional mitigating controls are needed. Access to perform disbursement transactions has been removed for the five state agency employees who were granted access by the bank.

In the future, anytime a migration occurs from one system to another at the bank, treasury staff will ensure all proper changes are made and only appropriate access is granted.

Person responsible: Deloris Staffanson, Agency Support Director
Joe Howe, Director of Treasury Operations, MMB

Implementation date: September 2010

**Recommendation – Finding 5**

The department should enhance the state's warrant special handling policy to address the risks related to obtaining pull warrants and wire transfer transactions.

The department should obtain appropriate and adequate authorization from state agencies before it allows warrants to be picked up or processes wire transfer transactions.

**Response**

Several procedures have been strengthened to address risks associated with pull warrants and wire transfer requests. Two signatures are now required on pull warrants for wire transfers.
The log for warrant pick-up is reviewed daily to ensure that authorized persons signed for the warrants. Phone verification of authorized persons is made when warranted. Department of Employment and Economic Development procedures have been modified to ensure authorization.

The other two issues related to the pull warrant process will be addressed in the near future:
The state policy for warrant special handling will be revised along with all other policies before the new SWIFT is implemented July 2011. Our list of agency authorized signatures will be updated.

Person responsible: Deloris Staffanson, Agency Support Director

Implementation date: October 2011

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

Sincerely,

Tom J. Hanson
Commissioner