OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial-Related Audit

Department of Finance
MAPS Interface Controls

NOVEMBER 7, 2002 **02-68**

Financial Audit Division

The Office of the Legislative Auditor (OLA) is a professional, nonpartisan office in the legislative branch of Minnesota State government. Its principal responsibility is to audit and evaluate the agencies and programs of state government (the State Auditor audits local governments).

OLA's 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 also investigates allegations that state resources have been used inappropriately.

The division has a staff of approximately fifty 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.

Consistent with OLA's mission, the Financial Audit Division works to:

- Promote Accountability,
- Strengthen Legislative Oversight, and
- Support Good Financial Management.

Through its Program Evaluation Division, OLA conducts several evaluations each year and one best practices review.

OLA is under the direction of the Legislative Auditor, who is appointed for a six-year term by the Legislative Audit Commission (LAC). The LAC is a bipartisan commission of Representatives and Senators. It annually selects topics for the Program Evaluation Division, but is generally not involved in scheduling financial audits.

All findings, conclusions, and recommendations in reports issued by the Office of the Legislative Auditor are solely the responsibility of the office and may not reflect the views of the LAC, its individual members, or other members of the Minnesota Legislature.

This document can be made available in alternative formats, such as large print, Braille, or audio tape, by calling 651-296-1727 (voice), or the Minnesota Relay Service at 651-297-5353 or 1-800-627-3529.

All OLA reports are available at our Web Site: http://www.auditor.leg.state.mn.us

If you have comments about our work, or you want to suggest an audit, investigation, evaluation, or best practices review, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us

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

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Ms. Anne Barry, Acting Commissioner
Department of Finance

We have conducted an information technology audit of selected components of the Minnesota Accounting and Procurement System (MAPS). The primary purpose of this audit was to determine if the Department of Finance had controls to protect the integrity and confidentiality of MAPS interface data. Our audit scope included a review of interface controls as of May 2002.

We conducted our audit in accordance with *Government Auditing Standards*, as issued by the Comptroller General of the United States. Those standards require that we obtain an understanding of management controls relevant to the audit. The standards also require that we design the audit to provide reasonable assurance that the Department of Finance complied with provisions of laws, regulations, contracts, and grants that are significant to the audit. The department's management is responsible for establishing and maintaining the internal control structure and complying with applicable laws, regulations, contracts, and grants.

This report is intended for the information of the Legislative Audit Commission and the management of the Department of Finance. This restriction is not intended to limit the distribution of this report, which was released as a public document on November 7, 2002.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: June 20, 2002

Report Signed On: November 4, 2002

Room 140, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651/296-4708 • Fax: 651/296-4712
E-mail: auditor@state.mn.us • TDD Relay: 651/297-5353 • Website: www.auditor.leg.state.mn.us

Table of Contents

Audit Participation

The following members of the Office of the Legislative Auditor prepared this report:

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Christopher Buse, CPA, CISA, CISSP	Information Technology Audit Manager
Mark Mathison, CPA, CISA	Auditor-in-Charge
Susan Kachelmeyer, CPA, CISA	Auditor

Exit Conference

We discussed the results of the audit with the following staff of the Department of Finance at an exit conference on October 29, 2002:

Anne Barry	Acting Commissioner
Lori Mo	Assistant Commissioner, Accounting Services
Carole Charbonneau	Assistant Commissioner, Administrative Services
Jean Henning	Chief Information Officer
Donna Visness	MAPS IS Director
Mary Bogie	Finance Services Director

Department of Finance
MAPS Interface Controls

Report Summary

Overall Audit Conclusions

The Department of Finance implemented controls to ensure that Interface Warrant Print (IWP) and Common Inbound Transaction Architecture (CITA) interface data is both accurate and complete. However, our audit identified two security weaknesses that should be addressed to further enhance IWP and CITA data integrity controls. The department also implemented controls to protect the integrity and confidentiality of Electronic Fund Transfer (EFT) data. However, we found several weaknesses that diminished the effectiveness of those controls.

Key Findings and Recommendations

- An inordinate number of state agency information technology professionals had unnecessary clearance to modify or delete another agency's CITA interface data. We recommended that the department restrict employees to their own agency's CITA interface data and log actions performed by information technology professionals with extremely powerful security clearances. (Finding 1, page 6)
- The department did not adequately secure a powerful Minnesota Accounting and Procurement System (MAPS) account. We recommended that the department secure powerful MAPS accounts so that unauthorized people cannot use them. Furthermore, we recommended limiting agencies to the minimum clearance that is needed to process their IWP and CITA interface batches. (Finding 2, page 7)
- The department did not have effective authentication controls for some accounts that have clearance to perform EFT functions. We recommended that the department enforce its policy that prohibits employees from sharing passwords and store its bank smart card in a secure location. Also, if passwords must be stored in a computer file, we recommend that the department limit access to that file and encrypt the file's contents. (Finding 3, page 10)
- The department transferred unencrypted EFT data over public networks, making it susceptible to eavesdropping. We recommended encrypting all EFT data that is transferred over public networks. (Finding 4, page 11)
- The department did not adequately separate EFT processing duties. We recommended that the department develop controls to detect EFT batch errors or irregularities before they are submitted to the state's financial institution for Automated Clearing House (ACH) processing. (Finding 5, page 11)

Background

This information technology audit assessed the adequacy of MAPS data interface controls. Most data that is processed by MAPS is captured through interfaces with other state agency computer systems. Totaling over $18.9 billion, IWP and CITA interface transactions accounted for approximately 73 percent of the state's expenditures during fiscal year 2002. EFT data files are one of the most significant outbound MAPS interfaces. During fiscal year 2002, the department disbursed over $12.2 billion through EFT.

Chapter 1. Introduction

This information technology audit assessed the adequacy of Minnesota Accounting and Procurement System (MAPS) data interface controls. MAPS is used by most state agencies to purchase goods and services, pay vendors, record accounting transactions, and prepare required financial reports. Most of the data that is processed by MAPS is not directly keyed into the system by state employees. Instead, this data is captured through interfaces with other state agency computer systems. Interfaces also pass some MAPS data back to certain state agency computer systems and financial institutions.

MAPS accepts incoming data through two types of interfaces: Interface Warrant Print (IWP) and Common Inbound Transaction Architecture (CITA). Table 1-1 describes each interface type.

Table 1-1
Comparison of MAPS Inbound Transaction Interface Types

Interface Type	Expenditure Transactions Accepted?	Revenue Transactions Accepted?
I W P	**Yes.** IWP interfaces capture expenditure data from computer systems that rely on MAPS for payment processing.	**No**
CITA	**Yes.** CITA interfaces capture expenditure data from many state agency computer systems. Systems that process their own payments, such as the state's central payroll system, typically use a CITA interface to pass data to MAPS	**Yes**

Source: Auditor prepared.

As illustrated in Table 1-2, approximately 65percent of the expenditure transactions recorded in MAPS during fiscal year 2002 entered the system through either an IWP or CITA interface. Totaling over $18.9 billion, these interface transactions accounted for approximately 73 percent of the state's expenditures for that period.

Table 1-2
MAPS Expenditures Summarized by Transaction Source
July 1, 2001, through June 30, 2002

Transaction Source	Number of Transactions	Percent of Total	Total Transaction Amount	Percent of Total
I W P Interfaces	14,414	0	$14,587,279,970	56
CITA Interfaces	3,458,715	65	4,337,167,803	17
Transactions Entered Into MAPS	1,843,911	35	6,985,998,811	27
Total	**5,317,040**	**100**	**$25,910,446,584**	**100**

Source: MAPS General Ledger.

Department of Finance
MAPS Interface Controls

The Department of Finance creates at least one distinct IWP or CITA interface for every state agency computer system that passes data to MAPS. As a result, some large state agencies with more than one major system have numerous IWP and CITA interfaces. Table 1-3 depicts the total number of IWP and CITA revenue and expenditure interfaces by state agency. It also identifies the total revenues and expenditures interfaced into MAPS during fiscal year 2002.

Table 1-3
Total IWP and CITA Interface Revenues and Expenditures By Agency
July 1, 2001, through June 30, 2002

Agency	Interface Type	Total Revenue	Total Expenditures	Number of Interfaces
Attorney General	IWP		$1,004,910	1
Children, Families & Learning	IWP		$5,424,174,421	2
Commerce	CITA	$9,999,987		1
Corrections	CITA	$4,264,589	$17,718,433	1
Human Services	CITA	$836,302,438	$968,313,771	8
Human Services	IWP		$5,307,197,396	6
Employee Relations	CITA	$19,723,869		1
Employee Relations	IWP		$9,650,311	2
Economic Security	IWP		$17,246,424	2
Finance	CITA	$151,826,143	$2,793,167,868	5
Housing Finance Agency	CITA		$71,934,009	1
Labor and Industry	IWP		$98,906,930	3
MN State Colleges & Universities	CITA	$622,330,862	$478,117,422	1
Minnesota State Retirement System	IWP		$381,003,536	3
Natural Resources	CITA	$141,499,176		1
Natural Resources	IWP		$1,379,691	1
Public Employees Retirement Association	IWP		$875,652,937	3
Public Safety	CITA	$1,161,823,807		3
Public Safety	IWP		$2,895,241	2
Revenue	CITA	$1,345,474	$7,916,299	2
Revenue	IWP		$1,041,866,224	4
Secretary of State	CITA	$868,019		1
Secretary of State	IWP		$1,030,341	1
Teachers Retirement Association	IWP		$954,506,373	2
Transportation	CITA	$1,176,853		2
Transportation	IWP		$470,765,236	1
Total		**$2,951,161,217**	**$18,924,447,773**	**60**

Source: MAPS General Ledger.

Department of Finance
MAPS Interface Controls

Electronic Fund Transfer (EFT) data files are one of the most significant outbound MAPS interfaces. To save time and administrative costs, the Department of Finance now uses EFT to pay many state vendors. In fact, during fiscal year 2002, the department disbursed over $12.2 billion through EFT. Each day, MAPS produces EFT data files. The Department of Finance uses special banking software to format, validate, and electronically transfer this EFT data to a major financial institution, where payment processing occurs.

Chapters 2 and 3 discuss the scope, objectives, and methodology that we used to assess the adequacy of MAPS interface controls. Chapter 2 addresses controls over IWP and CITA interfaces. Chapter 3 address controls over outbound EFT data transmissions. We obtained our evaluation criteria from the Control Objectives for Information and Related Technology (COBIT), published by the Information Systems Audit and Control Foundation. The COBIT Framework includes 34 high-level control objectives and 318 detailed control objectives, grouped in four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring.

Chapter 2. CITA and IWP Interface Controls

Chapter Conclusions

The Department of Finance implemented controls to ensure that IWP and CITA interface data is both accurate and complete. However, the department could further enhance its controls by remedying a security weakness that allows one agency to change another agency's interface data. The department also needs to limit access to one MAPS account that has extremely powerful security clearance.

Under state law, all state agencies must record their financial activities in the Minnesota Accounting and Procurement System (MAPS). This legal requirement poses significant challenges because MAPS is only one of many state computer systems that initiate accounting transactions. For example, state payments to medical providers are initiated by a computer system in the Department of Human Services, and payments to school districts are initiated by systems in the Department of Children, Families & Learning.

To eliminate the need for duplicate data entry, the Department of Finance developed two methods to interface accounting data into MAPS:

Common Inbound Transaction Architecture (CITA). State agencies can use CITA to interface most types of accounting transactions into MAPS. For example, some state agencies use CITA to interface revenue and expenditure data into MAPS. Computer systems that process their own payments also can use CITA to interface data.

Interface Warrant Print (IWP). State agency computer systems that rely on MAPS for payment processing must use an IWP interface. For example, a computer system managed by the Department of Human Services computes the amounts to be paid to all medical providers. The system passes this detailed expenditure data to MAPS, which processes the medical provider payments and posts summarized expenditure data to the general ledger.

The Department of Finance developed many controls to protect the integrity of CITA and IWP data. Of greatest significance, the department used security features in MAPS and a software package called ACF2 to restrict access to interface data. ACF2 security software controls access to all data that resides on the state's central mainframe computers. The department also subjects all CITA and IWP interface batches to a series of edits before processing payments or posting data to MAPS. Finally, the department developed MAPS screens and reports to help agencies monitor their IWP and CITA interface batches.

Department of Finance
MAPS Interface Controls

Audit Objective and Methodology

This portion of our audit assessed the adequacy of IWP and CITA interface controls. Specifically, we designed our work to answer the following question:

- Did the department implement controls to protect the integrity of IWP and CITA data and ensure that only valid data is posted to MAPS?

To answer this question, we interviewed information technology professionals in the Department of Finance who designed and oversee interface controls. We also used computer assisted audit tools to analyze and test ACF2 and MAPS security controls. Finally, we designed and processed IWP and CITA test batches to determine if key interface edit programs were functioning properly.

Conclusions

The Department of Finance has controls to ensure that data interfaced into MAPS is both accurate and complete. However, the department could further enhance its controls by addressing two security weaknesses that came to our attention. As discussed in Finding 1, insufficient security controls allow one agency to make unauthorized changes to another agency's interface data. In Finding 2, we discuss a powerful MAPS account that was not adequately secured.

Audit Findings and Recommendations

1. Some individuals had unnecessary clearance to IWP and CITA data.

The department did not deploy sufficient security controls over IWP and CITA interface data. While reviewing ACF2 security, we found an inordinate number of state agency information technology professionals with clearance to modify or delete another agency's CITA interface data. State agency employees only need clearance to their own agency's data to fulfill their job duties. We also found information technology professionals in the Department of Administration's Intertechnologies Group (InterTech) that had complete and unfettered access to all IWP and CITA data. We recognize that InterTech sometimes needs broad clearance to agency data to perform maintenance. However, logging these maintenance activities would give the department a mechanism to identify unauthorized data changes and other inappropriate events.

Recommendation

- *The department should restrict employees to their own agency's CITA interface data and log actions performed by information technology professionals with extremely powerful security clearances.*

2. One powerful MAPS account was not properly secured.

One agency used one of the department's most powerful MAPS accounts to process its interface batches. This account had clearance to modify or delete nearly all MAPS data and computer programs. Agencies that process interface batches only need clearance to read and modify specific MAPS files. Providing agencies with broader clearance than what is needed exposes all MAPS data to an unnecessary risk of loss.

Recommendations

- *The department should secure powerful MAPS accounts so that unauthorized people cannot use them.*

- *The department should only give agencies the minimum clearance that is needed to process their interface batches.*

Chapter 3. Electronic Fund Transfer Controls

Chapter Conclusions

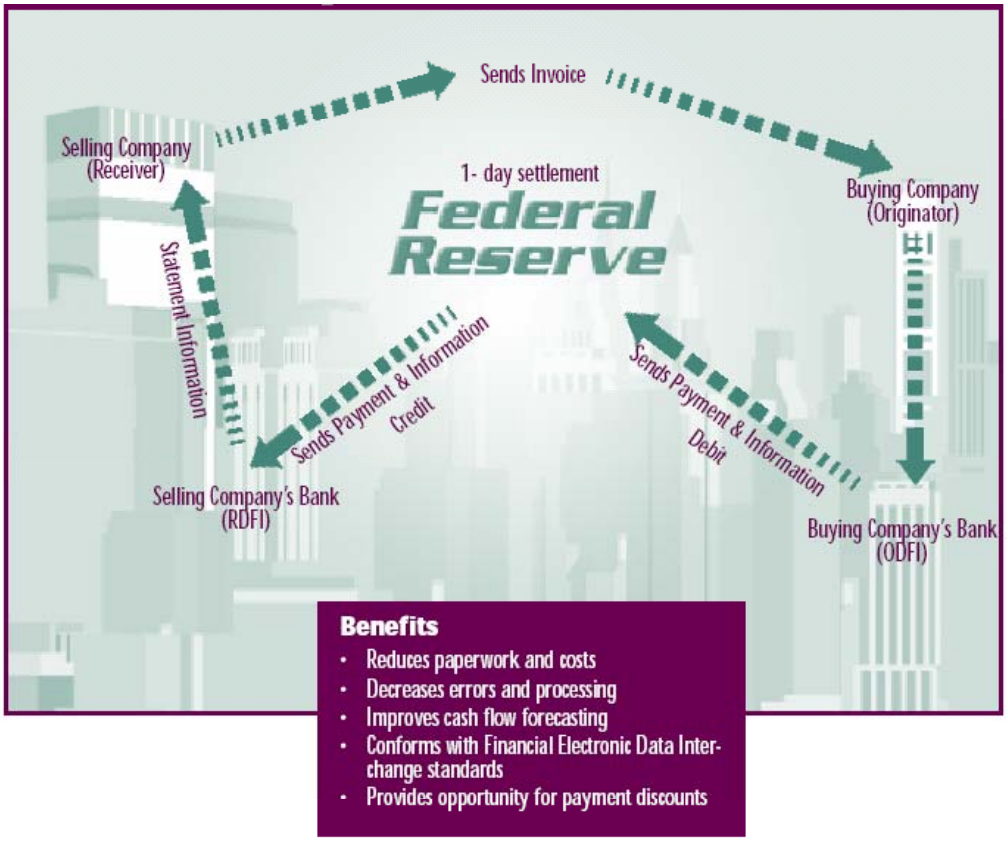
The department has implemented controls to protect the integrity and confidentiality of EFT data. However, several weaknesses diminished the effectiveness of these controls. Specifically, the department did not have adequate controls to confirm the identity of people who attempted to access the computer systems that house EFT data. The department also did not adequately protect EFT data that is transmitted over public networks. Finally, should inappropriate changes be made to EFT batches, the department may not detect those changes until the funds have been released from the state treasury.

To reduce costs, the Department of Finance has taken steps to pay more of its vendors through electronic funds transfer (EFT). During fiscal year 2002, the department gathered the necessary banking information to convert over 5,300 vendors to EFT. The department also made EFT payments totaling $12.2 billion during fiscal year 2002, an increase of $2.9 billion from the prior fiscal year.

The department uses the Automated Clearing House (ACH) network to make EFTs. As illustrated in Figure 3-1, the ACH network links the state's financial institution to those used by its vendors. Acting as the middleman, the Federal Reserve System clears all ACH transactions between these financial institutions. All transactions processed over the ACH network must comply with detailed rules, promulgated by the National Automated Clearing House Association.

Paying vendors through EFT offers enormous benefits. However, EFT payments also foster new risks that must be understood and managed. For example, organizations need strong security controls to protect EFT payment batches while they are being assembled. Organizations also need strong controls to protect EFT batches while they are being transmitted over networks.

Figure 3-1
Entities Involved in EFT Processing



Source: Federal Reserve System Publication.

Audit Objective and Methodology

This portion of our audit assessed the adequacy of EFT controls. Specifically, we designed our work to answer the following question:

- Did the department implement controls to protect the integrity and confidentiality of EFT data that is submitted to the state's financial institution for ACH processing?

To answer this question, we interviewed accounting and information technology professionals in the Department of Finance who manage EFT processing. We also obtained and analyzed security rules that protect EFT from unauthorized modification or disclosure. Finally, we searched for exploitable security weaknesses in the computers that are used by the department to prepare and transmit EFT batches.

Conclusions

Several weaknesses diminished the effectiveness of the department's EFT controls. Finding 3 discusses weaknesses in the department's computer system authentication controls. In Finding 4, we discuss weaknesses in the way that the department transmits EFT data over networks. Finally, in Finding 5, we discuss key EFT processing duties that were not properly separated.

Audit Findings and Recommendations

3. Accounts used for EFT processing were not properly secured.

The department does not have effective authentication controls for some accounts that have clearance to perform EFT functions. Most organizations rely on unique accounts and passwords to authenticate the identity of people who attempt to access their computer systems. This authentication approach is called "single factor" authentication because it places complete reliance on a secret password that should only be known by one person. Organizations that deploy highly sensitive computer systems often supplement secret passwords with additional authentication controls, such as smart cards or biometric devices. Authentication controls are extremely important because they limit computer system access to specific people. Authentication controls also provide organizations with a mechanism to trace specific computerized events to the person who initiated each event.

During our audit, we found one employee who used another employee's account and password to prepare an EFT payment batch. Sharing passwords is always unacceptable because it destroys individual accountability. Once a password has been compromised, it is virtually impossible to prove that a specific person initiated a specific computerized transaction. We also found a second EFT processing account and password that was stored in a computer file that could be accessed by many people. When questioned, the department immediately restricted access to that file. Finally, a group of employees had access to both the smart card and the secret password that are needed to access and transmit EFT data to the state's financial institution.

Recommendations

- *The department should enforce its policy that prohibits employees from sharing passwords.*
- *The department should store its bank smart card in a secure location.*
- *If passwords must be stored in a file, the department should limit access to that file and encrypt the file's contents.*

4. EFT file transfers were not adequately secured.

The department transferred unencrypted EFT data over public networks. Unfortunately, many tools allow unscrupulous people to capture transmissions that occur over public networks. Though encryption does not prevent eavesdropping, it makes it extremely difficult for hackers to decipher any hijacked transmissions.

During our audit, the department began encrypting some EFT data prior to transmission. However, additional work needs to be done to protect the remaining EFT data from eavesdropping.

Recommendation

- *The department should encrypt all EFT data that is transferred over public networks.*

5. EFT processing duties were not properly separated.

Two employees had clearance to prepare EFT batches, transmit those batches to the state's financial institution for ACH processing, and authorize the release of funds from the state treasury. At the time of our audit, an independent person did not verify the integrity of EFT batches before funds were released from the state treasury.

To improve controls, the department should develop procedures to ensure that individual employees cannot both perpetrate and conceal errors and irregularities. These procedures should be designed to detect EFT errors or irregularities before batches are submitted to the state's financial institution for ACH processing.

Recommendation

- *The department should develop controls to detect EFT batch errors or irregularities before they are submitted to the state's financial institution for ACH processing.*

November 1, 2002

James R. Nobles
Legislative Auditor
Office of the Legislative Auditor
1st Floor South-Centennial Building
658 Cedar Street
St. Paul, Minnesota 55155

Dear Mr. Nobles:

Thank you for the opportunity for my staff and I to discuss your audit findings with the people in your office responsible for the MAPS Interface Controls information technology audit. We are committed to providing accurate financial information to state agencies, the legislature, and the public and we take our responsibility for securing data and applications very seriously. We appreciate your work to identify opportunities to further enhance our security infrastructure. We will continue to work toward improvements in our processes.

Finding #1: Some individuals had unnecessary clearance to IWP and CITA data.

Recommendation

The department should restrict employees to their own agency's CITA interface data and log actions performed by information technology professionals with extremely powerful security clearances.

Response

We agree with this recommendation. In May 2002, we began logging and monitoring activity performed by information technology professionals with extremely powerful security clearances. This effort was completed in October 2002. In July 2002, we implemented a security change to restrict many CITA users to accessing their own agency's data, and are currently working with InterTech staff to resolve the remaining technical issues.

Person responsible: Steve Olson Estimated Completion Date: November 2002

Finding #2: One powerful MAPS account was not properly secured.

Recommendation

The department should secure powerful MAPS accounts so that unauthorized people cannot use them.

Response

We agree with this recommendation. The specific issue that was brought to our attention during the audit was resolved in July 2002. As an additional precaution, we have started monitoring files so we can detect instances of risk that may arise in the future.

Person responsible: Mary Kill Estimated Completion Date: Completed

Recommendation

The department should only give agencies the minimum security clearance that is needed to process their interface batches.

Response

We agree with this recommendation. We will research this issue further, and work closely with InterTech to explore and implement additional controls.

Person responsible: Donna Visness Estimated Completion Date: June 2003

Finding #3: Accounts used for EFT processing were not properly secured.

Recommendation

The department should enforce its policy that prohibits employees from sharing passwords.

Response

We agree with this recommendation. The need for confidential passwords has been addressed with the employees involved. As an additional precaution, we will periodically remind employees of the importance of following security procedures.

Person responsible: Paul Conery Estimated Completion Date: Completed

Recommendation

The department should store its bank smart card in a secure location.

Response

We agree with this recommendation. A bank smart card is no longer used to access and transmit EFT data to the state's financial institution. During the audit period, the department was in the process of converting from modem to web transmission of EFT data. In June 2002, the department began transmitting data using a secure web-based solution provided by the state's financial institution.

Person responsible: Paul Conery Estimated Completion Date: Completed

Recommendation

If passwords must be stored in a file, the department should limit access to that file and encrypt the file's contents.

Response

We agree with this recommendation. As noted in the audit report, when we were questioned about an account and password that was stored in a file that could be accessed by many people, we immediately restricted access to that file. Regarding the recommendation to encrypt the file's contents, we will review the EFT transfer process along with the capabilities of file encryption software, to determine and implement the best solution to this problem.

Person responsible: Donna Visness Estimated Completion Date: June 2003

Finding #4: EFT file transfers were not adequately secured.

Recommendation

The department should encrypt all data that is transferred over public networks.

Response

We agree with this recommendation. As discussed in our exit conference, there is one remaining area where file protection is needed. To accomplish this, we will explore alternatives for encrypting the files, and will work closely with InterTech to implement the best solution.

Person Responsible: Jayne Florek Estimated Completion Date: June 2003

Finding #5: EFT processing duties were not properly separated.

Recommendation

The department should develop controls to detect EFT batch errors or irregularities before they are submitted to the state's financial institution for ACH processing.

Response

We agree with this recommendation. Currently, the EFT batch is verified against the warrant register prior to submission. To address the need to adequately separate duties, we will explore alternatives to providing access to the EFT batch file prior to submission and implement a solution.

Person Responsible: Paul Conery Estimated Completion Date: November 2002

Sincerely,

/s/ Anne Barry

Anne Barry
Acting Commissioner

CC David Fisher, Department of Administration