OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial-Related Audit

Department of Employee Relations
Department of Finance
SEMA4 Information Technology Audit

AUGUST 29, 2002 **02-57**

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

Mr. Julien Carter, Commissioner
Department of Employee Relations

Ms. Pamela Wheelock, Commissioner
Department of Finance

We have conducted an information technology audit of select areas of the State Employee Management System (SEMA4). Our audit scope assessed the adequacy of selected computer general and application controls. The individual chapters of this report discuss the specific audit objectives and conclusions that we reached.

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

This report is intended for the information of the Legislative Audit Commission and the management of the Departments of Employee Relations and Finance. This restriction is not intended to limit the distribution of this report, which was released as a public document on August 29, 2002.

/s/ James R. Nobles	*/s/ Claudia J. Gudvangen*
James R. Nobles Legislative Auditor	Claudia J. Gudvangen, CPA Deputy Legislative Auditor

End of Fieldwork: August 12, 2002

Report Signed On: August 26, 2002

Department of Employee Relations
Department of Finance
SEMA4 Information Technology Audit

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	Audit Manager
Brad White, CPA, CISA	Audit Manager
Eric Wion, CPA, CISA	Auditor-In-Charge
Mark Mathison, CPA, CISA	Auditor
Sonya Johnson, CPA	Auditor
Kristen Peterson	Auditor
Heather White	Auditor
Gena Hoffman	Auditor

Exit Conference

We discussed the findings and recommendations with the following representatives of the Departments of Employee Relations and Finance at the exit conference held on August 22, 2002.

Department of Employee Relations:	
Steve Jorgenson	Chief Financial Officer
Laurie Hansen	Human Resources Services Manager
Department of Finance:	
Anne Barry	Deputy Commissioner
Carole Charbonneau	Assistant Commissioner, Administrative Services
Lori Mo	Assistant Commissioner, Accounting Services
Jean Henning	Chief Information Officer
John Vanderwenf	SEMA4 Technical Operations
Don Smith	Payroll Services Director

Department of Employee Relations
Department of Finance
SEMA4 Information Technology Audit

Report Summary

Overall Audit Conclusions

The Departments of Employee Relations and Finance have adequate controls to ensure that employees are paid the appropriate rates. Furthermore, the departments have adequate controls to ensure that the payroll is accurately processed and recorded in the state's general ledger. Finally, the departments have implemented controls to protect the integrity of SEMA4 payroll and personnel data. However, there are some opportunities to further enhance the security infrastructure.

Key Findings and Recommendations

- Some information technology professionals had excessive security clearances. Though some of these employees sometimes needed powerful clearances, we question the need to grant such clearances on a permanent basis. We recommend that the departments grant employees security clearances that are commensurate with their typical job duties and handle extraordinary security needs on a case-by-case basis (Finding 1).

- During transmission, some interface files were not appropriately secured. We recommend that the departments encrypt transmissions to and from SEMA4 (Finding 2).

Background

This information technology audit assessed the adequacy of key "application" and "general" controls of the State Employee Management System (SEMA4). Application controls filter out invalid data before it can be processed and ensure that remaining transactions are completely and accurately processed. General controls, such as security policies, procedures, and standards, are not unique to specific computerized business systems. Instead, they apply to all business systems that operate in a particular computing environment.

This page intentionally left blank.

Chapter 1. Introduction

This information technology audit assessed the adequacy of key "application" and "general" controls of the State Employee Management System (SEMA4). Application controls filter out invalid data before it can be processed and ensure that remaining transactions are completely and accurately processed. Application controls include both manual procedures, such as reconciliations, as well as computerized edit programs. General controls, on the other hand, are not unique to specific computerized business systems. Instead, they apply to all business systems that operate in a particular computing environment. Computer security policies, procedures, and standards are examples of general controls.

SEMA4 is an integrated human resource and payroll system that is used by over 100 state agencies. At the time of our audit, the system included detailed payroll and personnel records for approximately 49,000 current and 66,000 former employees. The system also maintains leave records for most state employees. During fiscal year 2002, the system processed nearly 5 million payroll and business expense transactions, resulting in a total expense of approximately $2.8 billion.

The system operates in a complex computing environment called "client server." The term client server refers to an environment where several different computers work together to accomplish a task. Typically, these computers communicate over a high-speed wide area network or the Internet. With SEMA4, state agency personal computers (i.e. the client) complete a significant portion of the computer processing. The remaining processing occurs on a central mainframe computer and on several other powerful computers called application servers. Communications between agency computers, the application servers, and the central mainframe occur over the State of Minnesota's wide area network.

Information technology professionals in the Departments of Employee Relations and Finance are responsible for maintaining the SEMA4 software. In general, the Department of Employee Relations provides technical support for personnel functions and the Department of Finance oversees payroll processing. However, due to the interrelationship between personnel and payroll activities, information technology professionals in the two departments must closely coordinate their efforts. They also must jointly establish procedures to prevent the unauthorized use, modification, or disclosure of SEMA4 data. To fulfill their responsibilities, the departments rely on assistance from the Department of Administration's InterTechnologies Group (InterTech). InterTech manages the state's central mainframe computing center and the wide area network. InterTech also manages the database that houses all of the SEMA4 data.

The primary audiences of this report are the Legislature and managers of the Departments of Employee Relations and Finance. However, we structured our conclusions to assist audit firms who will review payroll activities at the Minnesota State Colleges and Universities (MnSCU) system campuses. MnSCU is by far the largest employer in state government. At the time of our audit, MnSCU had over 12,000 active employees in SEMA4 and a payroll expense of $781 million for the period July 1, 2001, through June 30, 2002.

MnSCU developed its own human resource and leave management system, called the State Colleges and Universities Personnel/Payroll System (SCUPPS), to meet the unique needs of its faculty and administrators. SCUPPS transmits data to and receives data from SEMA4 on a regular basis. SCUPPS, rather than SEMA4, performs many critical control activities such as computing faculty and administrator biweekly gross pay amounts. Though SEMA4 ultimately processes the faculty and administrator payroll, it relies completely on critical application controls that are applied within SCUPPS. The total faculty and administrator payroll expense was approximately $579 million for the period July 1, 2001, through June 30, 2002.

Payroll, personnel, and leave records for MnSCU employees who are not faculty or administrators are subject to SEMA4 application controls. These application controls are the same controls that are applied to the rest of the state's workforce. For example, SEMA4 ensures that hourly pay rates assigned to employees fall within predefined ranges and that leave accrual rates are accurate. Total fiscal year 2002 payroll expense for MnSCU employees who were not faculty and administrators was approximately $202 million for the period July 1, 2001, through June 30, 2002.

Chapters 2 and 3 discuss the scope, objectives, and methodology that we used to assess the adequacy of key general and application controls. 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. SEMA4 Security Controls

Chapter Conclusions

The Departments of Employee Relations and Finance implemented security controls that protect the integrity of SEMA4 payroll and personnel data. However, there are some opportunities to further enhance the security infrastructure. Specifically, the departments should define information technology professionals' security clearances more precisely and encrypt file transfers to prevent eavesdropping.

Three security software packages work together to protect critical SEMA4 business data:

- **ACF2.** This software authenticates the identity of people who try to access the central mainframe computer. ACF2 also prevents unauthorized people from accessing the database and critical computer programs that underlie the SEMA4 system. Collectively, the Departments of Finance, Employee Relations, and Administration work together to define appropriate ACF2 security rules.
- **DB2.** When properly configured, DB2 security features prevent people from directly connecting to the database without using the appropriate SEMA4 screens. The Department of Administration's Intertechnologies Group (Intertech) manages DB2 security with input from the Departments of Employee Relations and Finance.
- **SEMA4 Security Profiles.** Customizable security features within SEMA4 limit people to the specific computer screens that they need to use to fulfill their job duties. The Department of Employee Relations manages SEMA4 security profiles. However, state agencies are responsible for determining the security needs of their employees who need to use the system.

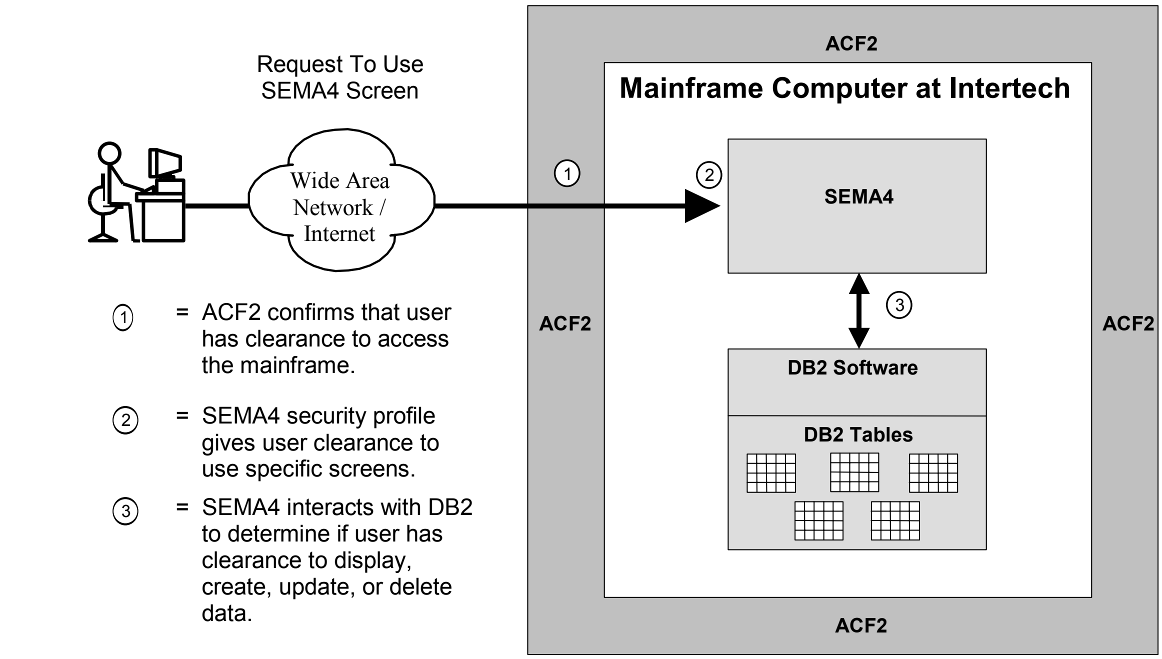
Figure 2-1 illustrates how ACF2, SEMA4 security profiles, and DB2 work together to control access to payroll and personnel screens and data.

Audit Objective and Methodology

Our general control work focused on the adequacy of SEMA4 security controls. Specifically, we designed our work to answer the following question:

- Did the departments design and implement controls to protect the integrity of critical SEMA4 payroll and personnel data?

Figure 2-1
Controlling Access to SEMA4 Payroll and Personnel Screens and Data


Request To Use
SEMA4 Screen
Wide Area
Network /
Internet
ACF2
Mainframe Computer at Intertech
1
2
SEMA4
3
ACF2
ACF2
DB2 Software
DB2 Tables
ACF2
1 = ACF2 confirms that user has clearance to access the mainframe.
2 = SEMA4 security profile gives user clearance to use specific screens.
3 = SEMA4 interacts with DB2 to determine if user has clearance to display, create, update, or delete data.

Source: Auditor Prepared.

To answer this question, we interviewed information technology professionals from the Departments of Finance, Employee Relations, and Administration. We also reviewed security documentation developed by the departments and provided by security software vendors. Finally, we used a variety of different computer-assisted auditing tools to analyze ACF2, DB2, and SEMA4 security data.

Conclusions

The Departments of Employee Relations and Finance implemented adequate security controls to protect critical payroll and personnel data. However, as discussed in Finding 1, some information technology professionals had more clearance than they needed to perform their typical job duties. Also, as discussed in Finding 2, some data transferred to and from SEMA4 was not encrypted to prevent eavesdropping.

The following table describes key security controls identified during our audit, tests that we performed to assess the adequacy of those controls, and our testing results.

Table 2-1
General Control Testing Summary

Control	Test Performed	Test Result
Predefined SEMA4 security profiles limit access to specific screens.	Examine selected security profiles to determine if they provide access to screens that would let employees perform incompatible system functions.	SEMA4 security profiles were designed to promote a separation of duties.
Extremely powerful security groups have been limited to certain employees who need such clearance.	Identify employees with powerful security profiles and determine if those people need such clearance.	Extremely powerful SEMA4 clearances were limited to certain employees who needed those clearances.
Supervisors must approve security requests.	Examine SEMA4 security changes to determine if properly authorized request forms supported those changes.	All SEMA4 security changes that we tested were properly authorized.
Database administrators can only perform DB2 database administration duties.	Determine if anyone other than DB2 administrators have clearance to perform powerful database administration functions.	In general, database administration privileges were limited to information technology professionals who needed such clearance to fulfill their job duties. Furthermore, all database maintenance activities were logged and reviewed.
Direct access to the DB2 database is limited to selected employees who need such clearance.	Identify who can directly connect to DB2 to update data tables and determine whether those people need such clearance.	Direct connections to DB2 were limited to certain information technology professionals who needed such clearance to fulfill their job duties. Activities performed by these individuals were logged and reviewed. However, as discussed in Finding 1, opportunities exist to improve controls.
ACF2 security features limit access to critical SEMA4 data and computer programs.	Examine ACF2 security rules to identify people who can access SEMA4 computer programs and data. Determine if those employees need such clearance to fulfill their job duties.	In general, ACF2 security rules limit access to SEMA4 data and computer programs. However, as discussed in Finding 1, opportunities exist to improve controls.

Department of Employee Relations
Department of Finance
SEMA4 Information Technology Audit

Current Findings and Recommendations

1. Some information technology professionals had excessive security clearances.

DB2 and ACF2 security features provided some computer programmers with clearance to update SEMA4 data and computer programs. Typically, programmers only work in test environments and are prohibited from accessing "production" programs and data. When questioned, supervisors told us that these information technology professionals sometimes need powerful clearances to perform periodic system maintenance. Supervisors also told us that actions performed by these information technology professionals were logged and reviewed. We recognize that information technology professionals sometimes need extremely powerful security clearances. However, granting such powerful clearances on a permanent basis creates an unnecessary security risk. To improve controls, the departments should temporarily grant powerful clearances to employees to perform certain tasks and revoke those access rights when the tasks are complete.

We also identified certain security weaknesses that could give unauthorized people with central mainframe accounts "read only" access to sensitive data. The departments need to remedy these security weaknesses to protect sensitive and confidential data from unauthorized disclosure.

Recommendations

- *The Departments of Employee Relations and Finance should grant employees security clearances that are commensurate with their typical job duties and handle extraordinary security needs on a case-by-case basis.*

- *The Departments of Employee Relations and Finance should work with Intertech to correct the security weaknesses that could provide unauthorized "read-only" access to data.*

2. Some interface files were not appropriately secured during transmission.

Some data transferred to and from SEMA4 was not encrypted. Data transfers to and from SEMA4 take place 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.

Recommendation

- *The Departments of Employee Relations and Finance should encrypt transmissions to and from SEMA4.*

Chapter 3. Application Controls

Chapter Conclusions

The Departments of Employee Relations and Finance implemented controls to ensure that employee pay rates are correct. The departments also have adequate controls to ensure that the payroll is accurately processed and recorded in the state's general ledger.

Application controls are controls over the input, processing, and output of data. Application controls are important because they help ensure that:

- only complete, accurate, and valid data is processed;
- all transactions are processed completely and accurately; and
- reports and other system outputs fulfill expectations.

Application controls include computerized edits and manual procedures, such as the review of computer generated exception reports.

The Department of Employee Relations has many controls to ensure that people are paid the appropriate rate. Of greatest significance, internal tables in SEMA4 outline the negotiated salary ranges for all jobs in state government. When agencies use the system to assign an employee to a job, SEMA4 ensures that the requested pay rate does not exceed the maximum for that job. SEMA4 has an "off-step" mechanism that allows certain employees to bypass normal pay rate controls. However, the department runs special reports to detect inappropriate use of off-step codes.

The Department of Finance has controls to verify the accuracy of the biweekly payroll processing. State agency payroll officers enter employees' hours worked and leave taken at the end of each pay period. SEMA4 uses this data to calculate the gross pay, deductions, and net pay for the state workforce. The system also posts accounting transactions to the Minnesota Accounting and Procurement System (MAPS), the state's general ledger system. Numerous internal tables in SEMA4 help control these processes. The department also produces many different reports to detect any processing errors before funds are disbursed to employees. Furthermore, the department performs important reconciliations to ensure that the payroll is accurately recorded in MAPS and that amounts actually disbursed to employees are accurate.

Audit Objectives and Methodology

Our application control work focused on the adequacy of pay rate and payroll processing controls. Specifically, we designed our work to answer the following questions:

- Did the departments implement adequate controls to ensure that employee pay rates are accurate?

- Did the departments implement adequate controls to ensure that the biweekly payroll is completely and accurately processed?

- Did the departments ensure that payroll activities are properly recorded in MAPS?

To answer these questions, we interviewed information technology professionals in the Departments of Finance and Employee Relations. We also reviewed relevant documentation and used computer-assisted audit tools to analyze and test significant controls.

Conclusions

The departments have controls to ensure that employees are paid at the proper rates and that the biweekly payroll is accurately and completely processed. Also, reconciliations help ensure that payroll activities are properly recorded in MAPS, the state's general ledger.

The following table describes key security controls identified during our audit, tests that we performed to assess the adequacy of those controls, and our testing results.

Table 3-1
Application Control Testing Summary

Control	Test Performed	Test Result
Internal SEMA4 tables ensure that employee pay rates do not exceed the maximum allowable amount for their particular job.	On a sample basis, verify that salary ranges for jobs in SEMA4's internal control tables agree with negotiated agreements.	Job salary ranges in SEMA4 internal tables were accurate.
	Determine if any employees had pay rates that exceeded the maximum allowable for their job.	Except for employees with special off-step codes, no employees had pay rates that exceeded the maximum allowed.
Certain off-step codes limit employees to the negotiated maximum rate for their particular job.	Identify all off-step codes with maximum rate controls and the employees with those codes. Verify that none of these employees exceeded the maximum pay rate for their particular job.	No employees with rate limiting off-step codes exceeded their maximum salary rate.
The departments produce reports and review off-step transactions.	Assess the adequacy of the off-step reports and the Department of Employee Relation's review process.	The off-step reports and review process were adequate.
Internal SEMA4 tables ensure that employee leave accrual rates do not exceed the maximum allowed by negotiated labor agreements.	Recalculate biweekly sick and vacation leave accruals to determine if any employees exceeded the maximum rate.	No employee's biweekly sick and vacation leave accrual rates exceeded the negotiated maximum.
The SEMA4 pay calculation program computes the gross pay for all employees.	Recompute gross pay for all employees for one year and investigate any differences with amounts derived by SEMA4.	SEMA4 properly computed gross pay for all employees.
Internal SEMA4 tables ensure that retirement contribution rates correspond with rates specified in law.	On a sample basis, verify that SEMA4 control table retirement contribution rates agree with the authorized rates.	Retirement contribution rates were accurate.
Internal SEMA4 tables ensure that tax rates correspond with rates specified in law.	Verify that SEMA4 control table state and federal income and FICA tax rates agree with the authorized rates.	SEMA4 tax rates were accurate.
The Department of Finance reconciles SEMA4 transactions to MAPS and the amount disbursed each pay period.	Review and assess the adequacy of the reconciliation process. Verify the reconciliation was performed each pay period and any significant differences were resolved.	The reconciliation process was adequate, performed each pay period, and any significant differences were resolved.

This page intentionally left blank.

Minnesota Department of Finance

DOER
State of Minnesota
Department of
Employee Relations

August 26, 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 our staff to discuss your audit findings with the people in your office responsible for the State Employee Management System (SEMA4) 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 are pleased by the many positive comments we heard from your staff at the exit conference, and we appreciate your work to identify opportunities to further enhance our security infrastructure. We will continue to work toward improvements in our processes.

Recommendation

The Departments of Employee Relations and Finance should grant employees security clearances that are commensurate with their typical job duties and handle extraordinary security needs on a case-by-case basis.

Response

As the audit reports notes, there are controls in place to detect updates to information that occur outside of normal processing. Even though the controls are in place, we are reviewing our security to make sure we grant security appropriately. We are removing authorities that are not needed on an on-going basis in our current system.

It is necessary to maintain powerful security clearances for selected employees that have responsibility to resolve problems within our application systems. Many of the problem resolutions occur after normal working hours and access must be available to them with little notice. We will evaluate alternative methods for addressing these needs as you have recommended. We will also continue to use our logging and detection reporting to monitor the changing of information by these employees. As job responsibilities and system requirements change, we will review security clearance for these employees and adjust their authority accordingly.

Person responsible: John Vanderwerf

Estimated completion dates: Removing unnecessary authorities: September 2002
Evaluation of alternative emergency access: March 2003

Recommendation

The Departments of Employee Relations and Finance should work with InterTech to correct the security weaknesses that could provide unauthorized "read-only" access to data.

Response

We will meet quarterly with InterTech to monitor and approve all security clearances authorized to manage the SEMA4 environment.

Person responsible: John Vanderwerf

Estimated completion date: October 2002

Recommendation

The Departments of Employee Relations and Finance should encrypt transmissions to and from SEMA4.

Response

We will investigate file encryption alternatives and work with MnSCU and our other interface partners to evaluate the available options, including the related implementation costs.

Person responsible: John Vanderwerf

Estimated completion date: April 2003

Sincerely,

/s/ Pamela Wheelock

Pamela Wheelock, Commissioner
Department of Finance

/s/ Julien C. Carter

Julien C. Carter, Commissioner
Department of Employee Relations