OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial-Related Audit

# Department of Employee Relations
# Department of Finance
## SEMA4 Information Technology Audit

AUGUST 28, 2003 03-47

# 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

Representative Tim Wilkin, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. Cal Ludeman, Commissioner
Department of Employee Relations

Mr. Dan McElroy, 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 the 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.

Information technology audits frequently include the review of sensitive security data that is legally classified as nonpublic under the Minnesota Data Practices Act. In some cases, to protect state resources and comply with the Minnesota Data Practices Act, we must withhold security-related details from our publicly released report. When these situations occur, we communicate all pertinent details to agency leaders in a separate, confidential document. For this audit, we issued a separate, confidential document to the management of the departments of Employee Relations and Finance.

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 28, 2003.

*/s/ James R. Nobles*

James R. Nobles
Legislative Auditor

*/s/ Claudia J. Gudvangen*

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: July 21, 2003

Report Signed On: August 25, 2003

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

**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 |
| Mark Mathison, CPA, CISA | Auditor-In-Charge |
| Patrick Ryan | 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 19, 2003:

Department of Employee Relations:

| | |
|---|---|
| Steve Jorgenson | Chief Information Officer |
| Laurie Hansen | Human Resources Division Manager |
| Elizabeth Houlding | Employee Insurance Division Manager |

Department of Finance:

| | |
|---|---|
| Dan McElroy | Commissioner |
| Anne Barry | Deputy Commissioner |
| Lori Mo | Assistant Commissioner, Accounting & Information Services |
| Jean Henning | Chief Information Officer |
| Don Smith | Payroll Services Director |
| John Vanderwerf | SEMA4 Technical 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, our audit identified some opportunities to further enhance the SEMA4 security infrastructure.

## Key Findings and Recommendations

- The departments did not revoke the SEMA4 security clearances of some individuals who left state service or transferred jobs. We recommend that the departments remove the unnecessary clearances, develop reports to help detect similar situations in the future, and search for automated ways to deactivate security clearances that are no longer needed (Finding 1, page 9).

- The departments did not actively monitor some SEMA4 system components for potential security breaches. We recommend that the departments deploy intrusion detection controls for all critical components of the system (Finding 2, page 9).

- The departments also were not properly monitoring some high-risk transactions. We recommend that they log and monitor changes to key human resource and benefit control tables and actively monitor correction transactions (Finding 3, page 14).

## Background

This information technology audit assessed the adequacy of key "application" and "general" controls of the State Employee Management System (SEMA4), which underwent a major upgrade in April 2003. 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 93 state agencies. During fiscal year 2003, the system processed payroll and personnel transactions for over 62,000 employees, resulting in total payroll and business expenses that exceeded $3 billion.

On April 7, 2003, the state implemented a new version of SEMA4 that takes full advantage of Internet technology. In the past, special software needed to be installed on the computers that accessed the system. Today, all that is needed is a web browser and access to the Internet. Virtually all SEMA4 processing occurs on a central mainframe computer and on several other powerful computers called application and web servers. Processing results are presented to the employees in the form of a web page.

Web technology has made SEMA4 accessible to many more individuals. However, it also has increased the complexity of the system and its underlying security infrastructure. At the time of our audit, over 70,000 people had access to SEMA4. This total now includes all state employees, who can access the system to view their paycheck information and perform other self-serve functions. Affiliated organizations, such as unions, charitable organizations, and retirement associations also can access the system to obtain payroll deduction and other information.

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.

## Department of Employee Relations
## Department of Finance
## SEMA4 Information Technology Audit

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. During the period July 1, 2002, through June 30, 2003, MnSCU had payroll expenses of $876 million for over 21,000 employees.

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 on critical controls that are applied within the SCUPPS environment. We recently conducted an audit of these controls and released our report, Legislative Audit Report 03-33, on June 19, 2003. The total faculty and administrator payroll expense was approximately $656 million during the period July 1, 2002, through June 30, 2003.

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. Payroll expense for MnSCU employees who were not faculty and administrators totaled approximately $220 million during the period July 1, 2002, through June 30, 2003.

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*

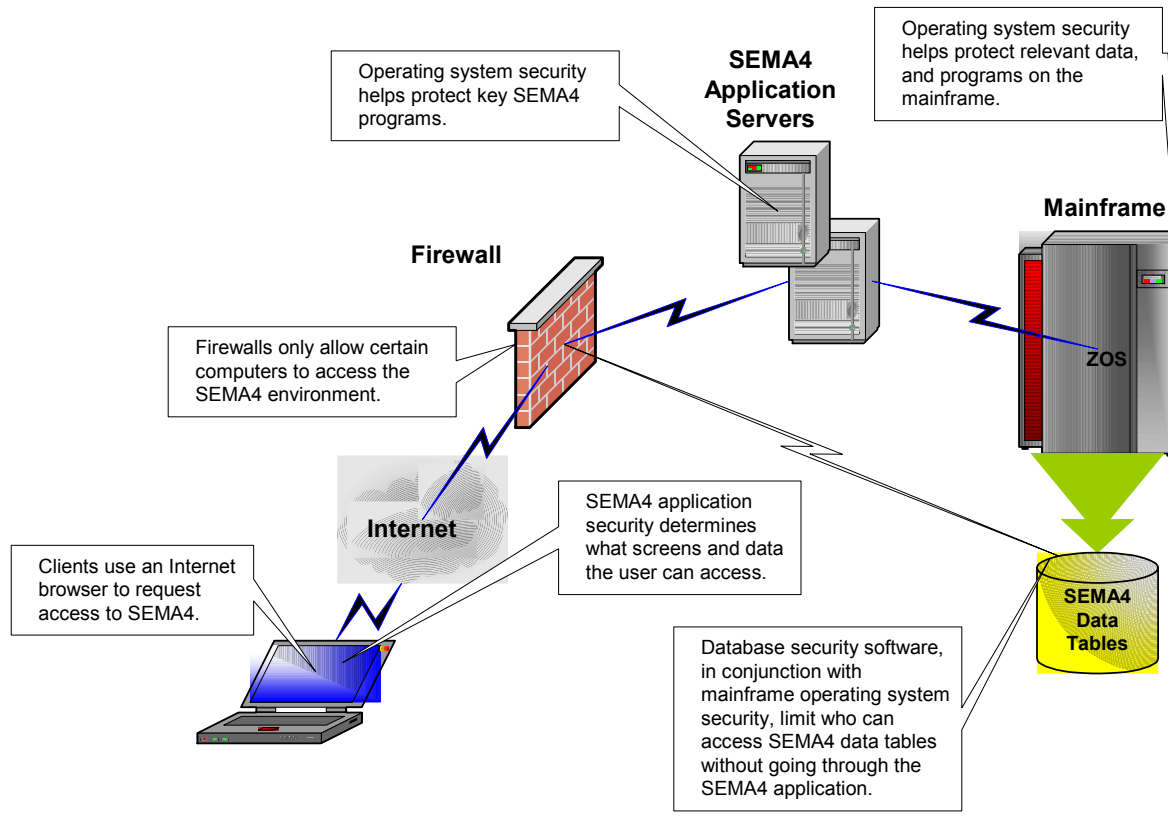
***The departments of Employee Relations and Finance implemented security controls that protect the integrity of SEMA4 payroll and personnel data. However, controls could further be enhanced by addressing two weaknesses that came to our attention. First, the departments did not revoke system access for some employees who left state service or transferred jobs. The departments also did not sufficiently monitor all aspects of the system for potential security breaches.***

Many security components work together to protect critical SEMA4 business data. The most critical security components include:

- **Operating System Security.** These software packages authenticate the identity of people who try to access the central mainframe computers and application servers. They also prevent 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 security rules.
- **Database Management System Security.** When properly configured, the database management security features prevent people from directly connecting to the database, which stores SEMA4 data and programs, without using the appropriate SEMA4 screens. The Department of Administration's Intertechnologies Group (Intertech) manages the database security with input from the departments of Employee Relations and Finance.
- **SEMA4 Application Security.** Customizable security features within SEMA4 assist in authenticating access to the application, limiting people to the specific computer screens that they need to use to fulfill their job duties, and limiting the data that a person can access. SEMA4 security profiles are centrally managed. However, state agencies are responsible for determining the security needs of their employees who need to use the system. Furthermore, the departments of Employee Relations and Finance determine the security needs of vendors and other nonstate agency users of the system.
- **Network and Perimeter Security.** Various firewalls and other network security components are used to encrypt data and limit which computers on the Internet can access the SEMA4 system.

Figure 2-1 illustrates how these security components work together to control access to payroll and personnel screens and data.

**Figure 2-1**
**Controlling Access to SEMA4 Payroll and Personnel**




Source: Auditor prepared.

## 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 a security infrastructure that protects the integrity of critical SEMA4 payroll and personnel data?

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 security data of the relevant operating systems, database management system, and the SEMA4 application.

## 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 individuals retained their SEMA4 access after transferring to another state agency or leaving state service. Also, as discussed in Finding 2, the departments did not actively monitor some SEMA4 components for potential security breaches.

Table 2-1 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 |
|---|---|---|
| Firewalls limit access to the SEMA4 environment to select computers. | Determine if firewall configurations are reasonable to limit admittance to the environment. | Firewalls were reasonably configured to limit access to SEMA4. |
| Account identifiers and secret passwords are used to authenticate authorized users of the system. | Determine if reasonable password management controls have been properly implemented. | Overall, password controls were reasonable to promote hard to guess passwords and require frequent changes. However, as noted in Finding 2, the departments can improve monitoring of certain computers. |
| Encryption technology prevents unscrupulous individuals from reading sensitive data as it passes on the Internet. | Verify that the departments have implemented industry standard encryption technology. | Sensitive SEMA4 data is encrypted during transmission. |
| Predefined SEMA4 security roles 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. | Overall, SEMA4 security roles were designed to promote a separation of duties. |
| SEMA4's row-level security limits people from accessing employee records outside of their agency/department. | Identify users of the system that can access HR and/or payroll data outside of their current employment agency and assess for appropriateness. | SEMA4 row-level security was appropriate to limit access to employment records based on job responsibilities. |

**Department of Employee Relations**
**Department of Finance**
**SEMA4 Information Technology Audit**

| Control | Test Performed | Test Result |
|---|---|---|
| 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. |
| Procedures have been implemented to disable SEMA4 access when a person leaves state service or transfers jobs. | Determine whether user accounts are timely disabled when a person leaves state service or transfers to another agency. | As noted in Finding 1, we identified 24 instances where individuals had inappropriate access after transfers or separations. |
| Only database administrators can perform database administration duties. | Determine if anyone other than database 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, database maintenance activities were logged and reviewed. |
| Direct access to the database management system is limited to selected employees who need such clearance. | Identify who can directly connect to the database management system and update data tables. Determine whether those people need such clearance. | Direct connections to the database 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. |
| Computer operating system security features limit access to critical SEMA4 data and computer programs. | Examine 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. | Computer operating security rules limit access to SEMA4 data and computer programs. |

## Current Findings and Recommendations

### 1. Some individuals retained their SEMA4 security clearances after leaving state service or transferring jobs.

Our audit identified 24 payroll or personnel officers with inappropriate security clearances. Eleven of the individuals still had system access even though they were no longer state employees. The remaining individuals transferred jobs to other state agencies, yet retained access to their prior agency's data.

Promptly removing or modifying security clearances is an important control to protect sensitive payroll and personnel data from unauthorized changes. We investigated these inappropriate security clearances and found outstanding issues from the recent system upgrade that may have allowed them to occur and go undetected. Of greatest significance, the departments have not developed new security reports for the upgraded system. As a result, since April 2003, state agencies have not had an effective mechanism to monitor who has access to their data. We also learned that some of the inappropriate clearances might have resulted from errors in the process used to convert security clearances to a new format required by the upgraded system. Specifically, we found that people whose access had been revoked prior to the conversion were inappropriately granted access under the new system.

Providing state agency security liaisons with timely reports will help detect inappropriate clearance in the future. However, we encourage the departments to pursue preventive control mechanisms as well. For example, the departments may want to consider developing a computerized process that inactivates the accounts of payroll and personnel officers who leave state service or transfer jobs.

*Recommendations*

- *The departments should deactivate the 24 accounts with inappropriate clearances.*
- *The departments should develop reports to help state agencies monitor who has access to their data.*
- *The departments should consider developing automated processes to inactivate powerful security clearances that are no longer necessary.*

### 2. The departments did not monitor some SEMA4 system components for potential security breaches.

Portions of the SEMA4 system lack sufficient controls to detect inappropriate activities, such as attacks by computer hackers. For some computers that we reviewed, the departments logged

certain security-related events, such as failed attempts to access the system. However, nobody consistently reviewed these logs for signs of irregularities. Prior to the recent SEMA4 upgrade, the departments had detective review processes for all critical system components. However, the addition of new system components and changes to the security infrastructure has led to certain monitoring lapses.

It is important to note that the departments have developed a robust security infrastructure with many controls to prevent inappropriate events from occurring. Unfortunately, though, history has shown that it is virtually impossible to design flawless preventive defenses. It is a sad reality that unscrupulous individuals discover new security exploits daily and use that knowledge to penetrate organizations with many layers of preventive defenses. This inherent security administration problem is why every organization must vigilantly monitor its systems for signs of attack.

*Recommendation*

- *The departments should deploy intrusion detection controls for all critical components of the SEMA4 system.*

# 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. However, the department did not monitor certain high-risk transactions for appropriateness, accuracy, and impact.***

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 completely and accurately processed; 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 foundation of the SEMA4 system was built and distributed by a well-known and reputable vendor, called PeopleSoft. The baseline PeopleSoft product comes standard with many embedded computerized edits, controls, and reports. Additional edits, controls, and reports were added or customized by information technology professionals who work for the departments of Employee Relations and Finance.

The Department of Employee Relations has many controls to ensure that people are paid the appropriate pay rates. Of greatest significance, internal tables in SEMA4 outline the negotiated salary ranges for most jobs in state government. When agencies use the system to assign an employee to a job, SEMA4 ensures that the pay rate agrees with these control tables. SEMA4 has an "off-step" mechanism that allows certain employees to bypass normal pay rate controls. However, the department runs special reports to monitor pay rates and the 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 processing errors before funds are disbursed to employees. Finally, 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. However, as discussed in Finding 3, the departments could improve controls by more closely monitoring certain high-risk transactions.

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. |
| The departments produce reports and review high-risk transactions. | Assess the adequacy of these reports and the review process. | In general, reports produced by the departments allow them to monitor a wide array of activities. However, as noted in Finding 3, additional monitoring of some high-risk transactions could further enhance controls. |
| Internal SEMA4 tables ensure that employee leave accrual rates do not exceed the maximum allowed by negotiated labor agreements. | On a sample basis, verify that employee leave accrual rates in SEMA4's internal control tables agree with negotiated agreements. Determine if any employees exceeded the maximum accrual rate. | Employee leave accrual rates in SEMA4 internal tables agree with negotiated agreements. Overall, the SEMA4 system accurately accrued sick and vacation leave for employees. |
| The SEMA4 pay calculation program computes the gross pay for all employees, except MnSCU faculty and administrators. | Recompute gross pay for all employees and investigate any differences with amounts derived by SEMA4 from conversion. | 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 that the reconciliation was performed each pay period and any significant differences were resolved. | An appropriate reconciliation process was performed each pay period and significant differences were resolved. |

### 3. The departments did not adequately monitor certain high-risk transactions.

The departments produce a wide array of reports to monitor the SEMA4 system. However, we identified two additional high-risk activities that should be reviewed to further enhance controls.

Changes made to some critical human resource and benefit control tables are not subject to independent oversight. In SEMA4, controls tables play a significant data integrity role by defining the rules that are used to validate payroll and personnel data. Unauthorized changes to these tables could lead to payments that do not comply with union bargaining agreements, tax laws, or other pertinent legal requirements. Recognizing their criticality, the departments implemented procedures to limit and monitor changes made to control tables through the database management system. However, this same level of scrutiny has not been applied to control table changes made through special SEMA4 screens.

The departments did not review correction mode transactions for appropriateness. SEMA4 provides many payroll and personnel officers with the ability to edit historical transactions. Though sometimes necessary, editing historical transactions is a very complex process that can cause unanticipated results in other parts of the system. This is particularly true for inexperienced employees who do not fully understand the interrelationships between payroll, personnel, and benefit processing. Reviewing correction mode transaction reports could help the department identify inappropriate transactions. It also could help identify recurring problems with the system and processing activities that are prone to error.

*Recommendation*

- *The departments should review changes to critical control tables and high-risk correction mode transactions.*

**Department of Employee Relations**
**Department of Finance**
**SEMA4 Information Technology Audit**

# Status of Prior Audit Issues
# As of July 21, 2003

## Most Recent Audit

**Legislative Audit Report 02-57**, issued August 29, 2002, assessed the adequacy of key application and general controls of the State Employee Management System (SEMA4). The report included two written findings related to security access and data transmission. We believe that the departments have taken the necessary steps to correct these issues.

**State of Minnesota Audit Follow-Up Process**

The Department of Finance, on behalf of the Governor, maintains a quarterly process for following up on issues cited in financial audit reports issued by the Legislative Auditor. The process consists of an exchange of written correspondence that documents the status of audit findings. The follow-up process continues until Finance is satisfied that the issues have been resolved. It covers entities headed by gubernatorial appointees, including most state agencies, boards, commissions, and Minnesota state colleges and universities. It is not applied to audits of the University of Minnesota, any quasi-state organizations, such as the metropolitan agencies, or the State Agricultural Society, the state constitutional officers, or the judicial branch.

*This page intentionally left blank.*

August 25, 2003

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. The April 2003 implementation of a major upgrade to the SEMA4 system was an important project for us which included a major transition to a new system architecture. 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.

**Finding**
**Some individuals retained their SEMA4 security clearances after leaving state service or transferring jobs.**

Recommendation: *The departments should deactivate the 24 accounts with inappropriate clearances.*

Response: This recommendation has been fully implemented; the 24 accounts have been deactivated.

Recommendation: *The departments should develop reports to help state agencies monitor who has access to their data.*

Response: In addition to an annual user access certification process that is required for all agencies, we have developed the recommended reports to help state agencies monitor access. By September 2003 we will complete distribution of policies and instructions to agencies on how to most effectively use these reports.
Person responsible: Laurie Hanson

Recommendation: *The departments should consider developing automated processes to inactivate powerful security clearances that are no longer necessary.*

Response: By December 2003 we will complete an analysis of the system modifications necessary to automate the security inactivation process as recommended, and evaluate the benefits of an automated approach compared to a manual process.
Person responsible: John Vanderwerf

**Finding**
**The departments did not monitor some SEMA4 system components for potential security breaches.**

Recommendation: *The departments should deploy intrusion detection controls for all critical components of the SEMA4 system.*

Response: During the time period of this audit, a temporary security solution was in place for some processes. Since audit field work was completed, users with the most powerful system access have been converted to our permanent security arrangement which provides additional protections for intrusion detection. In addition, we will immediately implement a process for reviewing critical access logs on a regular basis. By October 2003 we will further evaluate other options for intrusion detection.
Person responsible: John Vanderwerf

**Finding**
**The departments did not adequately monitor certain high-risk transactions.**

Recommendation: *The departments should review changes to critical control tables and high-risk correction mode transactions.*

Response: We will develop a process for additional oversight for human resource and benefit control table changes by November 2003. As you suggested, we intend to duplicate the process currently being used successfully to manage many payroll control table changes and will incorporate a supervisory approval process.

Your recommendation concerning a review process for correction mode transactions will require more analysis. By February 2004 we will analyze the number, type, and risk associated with the various types of correction mode transactions and develop a plan to minimize unanticipated results. Due to the variety in volume and impact of the different transaction types, we anticipate that a multi-prong solution will be warranted. Centralizing correction transactions for the highest risk processes will be considered, along with monitoring and training options.
Persons responsible: Laurie Hansen, Liz Houlding, and Don Smith

Thank you for the work you and your staff put into these helpful recommendations. It has been a pleasure to work with your excellent staff.

Sincerely,

*/s/ Dan McElroy*

Dan McElroy, Commissioner
Department of Finance

*/s/ Cal R. Ludeman*

Cal R. Ludeman, Commissioner
Department of Employee Relations