OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial Audit Division Report

Departments of Employee Relations, Finance, and Administration

SEMA4 Information Technology Audit

AUGUST 31, 2004 **04-36**

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 forty 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.

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 651-296-1235 (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, or evaluation, 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

Ms. Peggy Ingison, Commissioner
Department of Finance

Mr. Brian Lamb, Commissioner
Department of Administration

We have conducted an information technology audit of the State Employee Management System (SEMA4). The purpose of our audit was to assess the adequacy of selected computer controls as of June 2004. The Report Summary highlights our overall conclusions. Specific audit objectives and conclusions are contained in the individual chapters of this report.

We designed this audit to supplement other payroll audit work done by our office and certified public accountants engaged by the Minnesota State Colleges and Universities.

We conducted our audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we obtain an understanding of management controls relevant to the audit objectives. We used the guidance contained in *Control Objectives for Information and Related Technologies*, published by the IT Governance Institute, as our criteria to evaluate controls. We also obtained evaluation criteria from policies and procedures adopted by management and publications from hardware and software manufacturers whose products are part of SEMA4.

Government Auditing Standards require that we plan the audit to provide reasonable assurance that the departments complied with financial-related legal provisions that are significant to the audit. In determining the departments' compliance with legal provisions, we considered requirements of laws, regulations, contracts, and grant agreements.

To meet our audit objectives, we interviewed information technology and business professionals who oversee the systems and its controls. We also used computer-assisted audit tools to test selected controls.

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, Finance, and Administration.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: July 29, 2004
Report Signed On: August 27, 2004

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	Audit Manager
Mark Mathison, CPA, CISA	Auditor-In-Charge
Patrick Ryan	Auditor
Sally Tefera	Intern

Exit Conference

We discussed the findings and recommendations with the following representatives of the departments of Employee Relations, Finance, and Administration at the exit conference held on August 24, 2004:

Department of Employee Relations:

Cal Ludeman	Commissioner
Steve Jorgenson	Chief Information Officer
Laurie Hansen	Human Resources Division Manager
Liz Houlding	Employee Insurance Division Manager

Department of Finance:

Peggy Ingison	Commissioner
Lori Mo	Assistant Commissioner, Accounting and Information Services
Jean Henning	Chief Information Officer
John Vanderwerf	SEMA4 Technical Director

Department of Administration:

Jack Yarbrough	Assistant Commissioner, InterTechnologies Group
Jim Steinwand	Security Services Manager, InterTechnologies Group
Judy Hunt	Director, Internal Audit

Departments of Employee Relations, Finance, and Administration
SEMA4 Information Technology Audit

Report Summary

Key Conclusion:

The departments of Employee Relations and Finance implemented controls to ensure that employee pay rates are correct, and that payroll is accurately processed and recorded in the state's accounting system. The departments also worked with the Department of Administration to implement security controls that protected the integrity of SEMA4 payroll and human resources data.

Key Finding:

- The departments did not have appropriate controls to authenticate the identity of many people with access to SEMA4's self-service environment, where employees can enter various payroll and personnel information. As a result, it would be easier for unscrupulous persons to potentially guess passwords and gain access to the system. (Finding 1, page 11)

The audit report contained five findings relating to computer security weaknesses.

Audit Scope:

Audit Period:
As of June 2004

Selected Audit Areas:
- Security Controls
- Application Controls

Background:

This information technology audit assessed the adequacy of key controls over the State Employee Management System (SEMA4). SEMA4 is an integrated human resources and payroll system that is used by more than 90 state agencies. During fiscal year 2004, the system processed payroll and human resources transactions for over 62,000 employees, resulting in total payroll and business expenses that exceeded $3 billion.

The Department of Employee Relations provides support for human resources functions, and the Department of Finance oversees payroll processing for the entire state. Information technology professionals in these two departments work closely to maintain the SEMA4 system. To fulfill their responsibilities, the departments rely on assistance from the Department of Administration's InterTechnologies Group.

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.

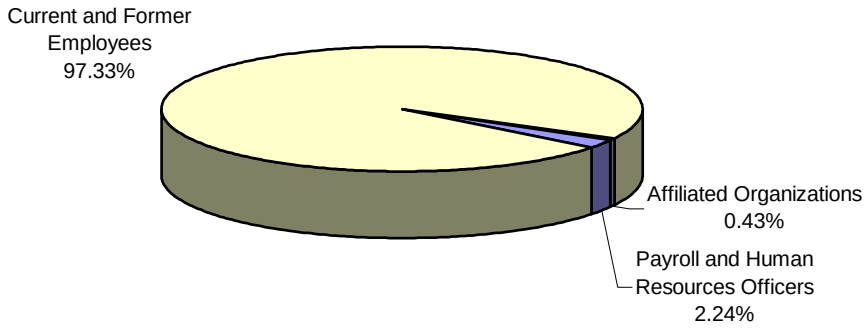
SEMA4 is an integrated human resources and payroll system that is used by more than 90 state agencies. During fiscal year 2004, the system processed payroll and human resources transactions for over 62,000 employees, resulting in total payroll and business expenses that exceeded $3 billion.

In April 2003, the state implemented a new version of SEMA4 that took full advantage of Internet technology. Implementation of this web-based version of SEMA4 significantly increased the number of people with access to the system. In the past, access was limited to state agency payroll and human resources officers. Today, all current and many former employees with an Internet connection and web-browser can access the system's "self-service" environment to:

- view payroll advices, leave balances, and W-2 forms;
- change benefit and demographic data;
- enter hours worked and leave taken; and
- approve timesheets submitted by subordinates.

Over 81,000 people had access to SEMA4 at the time of our audit. As illustrated in Figure 1-1, over 97 percent of these people were current and former employees with clearance to the self-service environment. Slightly over two percent of the people cleared to use the system were state agency payroll and human resources officers. The remaining people with clearance to SEMA4 worked for affiliated organizations, such as unions, charitable organizations, and retirement associations.

Figure 1-1
Groups of People With Clearance to SEMA4
As of June 2004



Source: Auditor prepared from SEMA4 security data.

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 human resources functions, and the Department of Finance oversees payroll processing. However, due to the interrelationship between human resources 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 and performs many security-related functions that impact the integrity of the environment.

The primary audiences for this report are the Legislature and managers of the departments of Employee Relations, Finance, and Administration. However, we structured our report to assist audit firms who will review payroll activities at the Minnesota State Colleges and Universities (MnSCU). MnSCU is by far the largest employer in state government. During the period July 1, 2003, through June 30, 2004, MnSCU had payroll expenses of $881 million for over 21,000 employees.

MnSCU developed its own human resources 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 SCUPPS 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, 2003, through June 30, 2004.

Payroll, human resources, and leave records for MnSCU employees who are not faculty or administrators are subject to SEMA4 controls. These 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 $225 million during the period July 1, 2003, through June 30, 2004.

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.

This page intentionally left blank.

Chapter 2. SEMA4 Security Controls

Chapter Conclusions

The departments of Employee Relations, Finance, and Administration implemented security controls that protect the integrity of SEMA4 payroll and human resources data. However, addressing five weaknesses that came to our attention could further enhance controls:

- ***The departments did not have appropriate controls to authenticate the identity of people with access to the SEMA4 self-service environment.***
- ***Three improperly configured security roles provided some people with inappropriate access to data.***
- ***The departments did not log or monitor activities performed by some information technology professionals with powerful security clearances.***
- ***Some accounts with access to the database management system may have excessive security clearances.***
- ***The departments did not take appropriate action against three agencies that did not comply with a SEMA4 security policy.***

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 computer, application servers, and web 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.

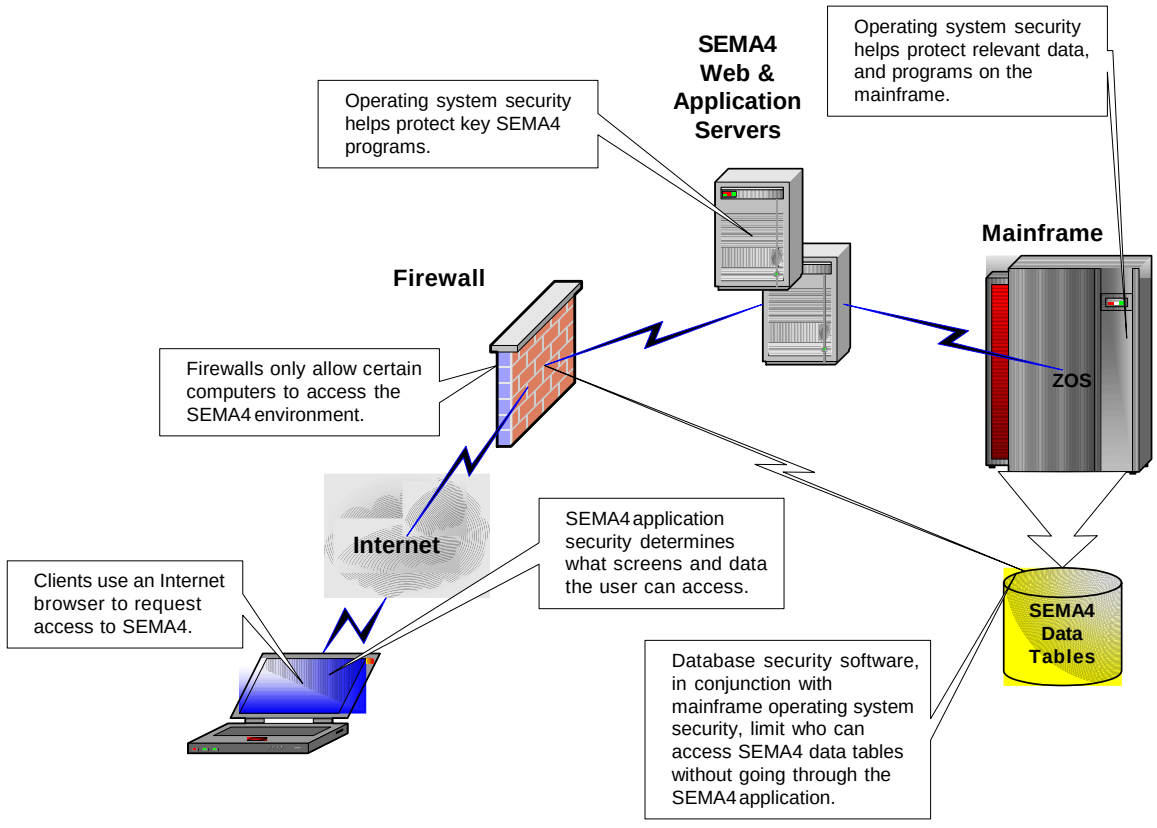
- **SEMA4 Application Security.** Customizable security features within SEMA4 assist in authenticating access to the application, limiting people to the specific computer screens that they need to use to fulfill their job duties, and limiting the data that a person can

access. SEMA4 security roles are centrally managed. However, state agencies are responsible for determining the security needs of their employees who use 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 system.

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

Figure 2-1
Controlling Access to SEMA4 Payroll and Human Resources



Source: Auditor prepared.

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 human resources data?

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. Findings 1 to 5 discuss weaknesses we identified, along with recommendations to further improve the security infrastructure.

Table 2-1
General Control Testing Summary

Control	Test Performed	Test Result
Security features in firewalls, operating systems, and other devices limit access to SEMA4.	Determine if firewall configurations appropriately limited access to the environment. Perform a vulnerability scan of selected devices to search for security weaknesses.	Firewall and operating system security features were properly configured to limit access to SEMA4.
IT professionals periodically scan SEMA4 devices to search for exploitable security weaknesses.	Ensure that IT professionals performed periodic scans and resolved any weaknesses that were identified.	IT professionals periodically scanned the environment and remedied security weaknesses.
Collectively, unique user accounts and secret passwords authenticate the identity of people with access to SEMA4.	Determine if robust password management controls have been implemented.	In general, the departments deployed adequate password controls for payroll and human resources officers. However, as noted in Finding 1, our audit identified 60 people with access to payroll and human resources data that could circumvent the standard password controls. We also found that the departments did not have sufficient controls to authenticate the identity of employees who access the self-service environment.
Encryption technology prevents unscrupulous individuals from reading sensitive data transmitted over the Internet.	Verify that the departments have implemented industry standard encryption technology.	Prior to transmission, sensitive SEMA4 data was encrypted using industry standard technology.
Predefined SEMA4 security roles limit people's access to specific screens.	Examine selected security roles to determine if they provide access to screens that can be used to perform incompatible system functions.	Overall, SEMA4 security roles were designed to promote a separation of duties. However, as noted in Finding 2, three inquiry-only roles erroneously gave employees clearance to update data.
SEMA4 security features limit most people to their own agency's records.	Identify users with statewide access to data and assess for appropriateness.	Most system users could only access their own agency's data. System users with statewide access to SEMA4 data needed such clearance to fulfill their job duties.

Departments of Employee Relations, Finance, and Administration
SEMA4 Information Technology Audit

Control	Test Performed	Test Result
Extremely powerful security roles are only given to certain employees who need such clearance.	Identify employees with powerful security roles and determine if those people need such clearance.	Extremely powerful SEMA4 clearances were limited to certain employees who needed those clearances.
For payroll and human resources officers, procedures are in place to disable SEMA4 access when a person leaves state service or transfers jobs.	Determine whether user accounts are promptly disabled when a person leaves state service or transfers to another agency.	Security clearances are promptly disabled for payroll and human resources officers that leave state service or change jobs.
A formal approval process exists to request access to SEMA4.	On a sample basis, verify that appropriate personnel approve access requests.	Access to SEMA4 was approved by designated security liaisons.
All security clearances are periodically recertified to confirm their validity.	Verify that security clearances were recertified.	In January 2004, the departments asked all state agencies to recertify their employees' SEMA4 clearances. However, as discussed in Finding 5, three state agencies did not comply with this request. Also, as discussed in Finding 4, some powerful database privileges were not periodically reviewed.
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. However, as discussed in Finding 4, some people and software accounts with extremely powerful database privileges may not need that level of clearance.
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 limited access to SEMA4 data and computer programs. However, as noted in Finding 3, updates and changes to some critical programs and data were not always logged and reviewed.

Current Findings and Recommendations

1. The departments did not adopt strong password controls for many people with access to SEMA4's self service environment.

The departments did not deploy automated controls to force people with access to the SEMA4 self-service environment to change their passwords. Instead, the departments gave employees default passwords and provided step-by-step instructions to change them to more secure secret passwords. Most employees never followed these instructions. In fact, we found over 56,000 employees whose passwords were still the defaults.

At the inception of the self-service environment, the departments made a decision not to enforce password changes or deploy other typical password controls. The justification for this decision was that all information in the environment was public and employees could only view the data. These two assumptions became obsolete as the departments added more functionality to the self-service environment. For example, employees now use the environment to enter timesheets and update confidential demographic data. Supervisors also can use the environment to approve timesheets electronically. When these functionality changes occurred, the departments did not make corresponding changes to the security infrastructure to address the new risks.

Our audit also identified 60 accounts, used primarily by payroll and human resources officers, which could circumvent the departments' password change policy. SEMA4 users with payroll and human resources clearances must change their passwords every 30 days. Most of these 60 accounts only required password changes every 90 days, and some did not require passwords to be changed at all.

Most organizations rely on unique user accounts and passwords to enforce two fundamental security principles: 1) positively confirming the identity of system users and 2) always having a mechanism to trace critical activities to specific individuals. Password control weaknesses make it difficult to confirm the legitimacy of SEMA4 users, thereby exposing payroll and human resources data to unnecessary risks.

Recommendation

- *The departments should implement strong password controls to make it more difficult for hackers to assume the identity of legitimate system users.*

2. Three improperly configured security roles provided some people with inappropriate access to data.

Three security roles, designed to give people inquiry-only access to data, inadvertently gave them the ability to add or change some sensitive data. Two of these security roles gave approximately 50 people the ability to add nonstate employees to SEMA4 and adjust their health

insurance eligibility status. The other security role gave 42 people clearance to process payroll adjustment transactions. To improve controls, the department should correct the configuration errors in these three security roles.

Recommendation

- *The departments should remove the update abilities from the identified inquiry-only security roles.*

3. The departments did not monitor some high-risk security events.

The departments do not log or monitor activities performed by some information technology professionals with powerful security clearances. Information technology professionals sometimes need direct access to the data underlying SEMA4 to perform maintenance functions. However, we found some cases where these types of maintenance activities were not logged or reviewed by an independent person. Without independent oversight, inappropriate changes to payroll or human resources data could occur and go undetected.

Recommendation

- *The departments should log and review data maintenance done by information technology professionals with powerful security clearances.*

4. Some accounts with access to the database management system may have excessive security clearances.

The Department of Administration's InterTechnologies Group (InterTech) has not thoroughly evaluated the appropriateness of all accounts with extremely powerful security clearances to the SEMA4 database. Information technology professionals responsible for managing a database environment typically need special clearance or "privileges" to do their work. Most database management systems offer a wide array of privileges to help organizations give information technology professionals the precise level of security clearance that they need to do their work. Some privileges only give information technology professionals the ability to perform specific tasks. Other privileges give information technology professionals complete access to perform any task, including changing any data and even deleting the entire database.

InterTech granted the most powerful database privilege to all members of its database team. It also granted this privilege to some accounts used by software products. Of these 20 accounts, 4 belonged to people that could no longer access the state's mainframe. When questioned, the department could not justify why all of these accounts needed the most powerful privilege when many less powerful and lower risk privileges were available.

Recommendation

- *InterTech should periodically evaluate and justify the need for accounts with powerful database security privileges.*

5. The departments did not take appropriate action against three agencies that did not comply with a SEMA4 security policy.

All state agencies must recertify their employees' SEMA4 security clearances annually. This policy helps ensure that people with access to sensitive payroll and human resources data continue to need that clearance to fulfill their job duties. The departments sent all state agencies the last recertification request on December 18, 2003. The departments gave state agencies until January 31, 2004, to review, update, and return the enclosed security reports. However, as of June 2004, the following three state agencies still had not returned the requested information:

- Minnesota State Colleges and Universities;
- Department of Natural Resources; and
- Department of Veterans Affairs.

Collectively, these three agencies account for approximately 24 percent of the people with clearance to view and update payroll and human resources data.

When questioned, SEMA4 security officers told us that they had made repeated attempts to obtain the required security data from each of these agencies. However, they did not have an escalation process in place to deal with agencies that simply did not comply. To improve controls, we encourage the departments to develop such escalation procedures. Direct communications from the executive leaders of the departments of Finance and Employee Relations to the leaders of agencies not in compliance may be one potential solution.

Recommendation

- *The departments should develop procedures to deal with state agencies that do not comply with established security policies.*

This page intentionally left blank.

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 accounting system.

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 properly 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.

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?

Table 3-1 describes key application 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's internal tables were accurate.
The departments produce and review reports designed to identify high-risk transactions.	Assess the adequacy of these reports and the review process.	Reports produced by the departments allow them to monitor a wide array of activities to detect errors and irregularities.
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.	Employee leave accrual rates in SEMA4's internal tables agree with negotiated agreements.
The SEMA4 pay calculation program computes the gross pay for all employees, except MnSCU faculty and administrators.	For material earning types, recalculate gross pay for all employees 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's control table retirement contribution rates agree with the authorized rates.	SEMA4 retirement contribution rates were accurate.

Departments of Employee Relations, Finance, and Administration
SEMA4 Information Technology Audit

Control	Test Performed	Test Result
Internal SEMA4 tables ensure that tax rates correspond with rates specified in law.	Verify that SEMA4's control tables contain state and federal income and FICA tax rates that are consistent with statutory rates.	SEMA4 tax rates were accurate.
Internal SEMA4 tables ensure the accuracy of employer and employee insurance rates.	Verify that SEMA4's controls tables are consistent with negotiated health and dental rates.	SEMA4 health and dental 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.

This page intentionally left blank.

Status of Prior Audit Issues
As of June 29, 2004

Most Recent Audit

Legislative Audit Report 03-47, issued August 28, 2003, assessed the adequacy of key application and general controls of the State Employee Management System (SEMA4). The report included three written findings related to system access and monitoring of the environment. We believe that the departments have taken the necessary steps to correct the specific issues identified. However, as discussed in our current Finding 3, additional monitoring weaknesses were identified.

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 26, 2004

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 to discuss with your staff the findings related to your 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. All of your written recommendations have been implemented or are in progress as detailed below. In addition, we are in the process of analyzing the verbal recommendations received from your staff and we will continue to work toward improvements in our processes.

1. Finding
The departments did not adopt strong password controls for many people with access to SEMA4's self-service environment.

Recommendation: *The departments should implement strong password controls to make it more difficult for hackers to assume the identity of legitimate users.*
Response: We agree. This recommendation has been fully implemented. Effective August 19, 2004, we have strengthened the SEMA4 password controls for the employee self-service environment. We have reduced the maximum logon attempts, increased minimum password length, and implemented expiration controls to force periodic password changes. The 60 accounts with password change requirements greater than 30 days have been corrected.
Agency Responsible: Employee Relations and Finance

2. Finding
Three improperly configured security roles provided some people with inappropriate access to data.

Recommendation: *The departments should remove the update abilities from the identified inquiry-only security roles.*
Response: We agree. This recommendation has been fully implemented. The three security roles have been changed to provide view only access.
Agency Responsible: Employee Relations and Finance

3. Finding
The departments did not monitor some high-risk security events.

Recommendation: *The departments should log and review data maintenance done by information technology professionals with powerful security clearances.*

Response: We agree. This recommendation is partially implemented. The Departments of Finance, Employee Relations and Administration have taken steps to address this recommendation. Security rules for production files in Finance and Employee Relations have been modified to log unplanned update activity. The Department of Administration is in the process of implementing a new security grouping that will reduce the number of information technology professionals with powerful clearances to SEMA4 information. The changes necessary to complete this regrouping will be completed by October 2004.

In addition, the three departments will evaluate security rules to determine where additional logging should be done and implement changes where appropriate. They will jointly re-evaluate security logging by November 2004 to determine if any additional changes are required.
Agency Responsible: Administration, Employee Relations and Finance
Persons Responsible: John Vanderwerf
Jim Steinwand

4. Finding
Some accounts with access to the database management system may have excessive security clearances.

Recommendation: *InterTech should periodically evaluate and justify the need for accounts with powerful database security privileges.*

Response: We agree. This recommendation will be fully implemented by August 31, 2004. We have implemented an annual recertification process for access privileges and revised our employee Data Practices Agreement regarding the need to access data. These actions will ensure better management and control the evaluation and justification process of accounts' database security privileges. Also, an analysis of the need for current access privileges of ITG employees has been completed and a determination made that they are appropriate.

This analysis will be repeated annually or when new releases of operating system and database system software are installed.
Agency Responsible: Administration
Persons responsible: Jim Steinwand

5. Finding
The departments did not take appropriate action against three agencies that did not comply with a SEMA4 security policy.

Recommendation: *The department should develop procedures to deal with state agencies that do not comply with established security policies.*

Response: We agree. This recommendation has been fully implemented. We have modified our procedures to include a process to escalate our request to increasingly higher levels of management as necessary to achieve compliance with the security policy. We have followed this new procedure with the three agencies that did not respond to our 2004 security recertification and we have now received the completed documents from the three agencies.
Agency Responsible: Employee Relations and Finance
Person responsible: Laurie Hansen

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,

Peggy S. Ingison, Commissioner
Department of Finance

Cal R. Ludeman, Commissioner
Department of Employee Relations

Brian J. Lamb, Commissioner
Department of Administration