Minnesota Accounting and Procurement System
Minnesota Statewide Employee Management System

Selected Scope Financial Audit
For the Period July 1, 1995, through March 31, 1996

September 1996

This document can be made available in alternative formats, such as large print, Braille, or audio tape, by calling 296-1235.

Financial Audit Division
Office of the Legislative Auditor
State of Minnesota

96-39

Centennial Office Building, Saint Paul, MN 55155 ● 612/296-4708

STATE OF MINNESOTA
OFFICE OF THE LEGISLATIVE AUDITOR
CENTENNIAL BUILDING, 658 CEDAR STREET • ST. PAUL, MN 55155 • 612/296-4708 • TDD RELAY 612/297-5353
JAMES R. NOBLES, LEGISLATIVE AUDITOR

Representative Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Ms. Laura King, Commissioner
Department of Finance

Ms. Elaine Hansen, Commissioner
Department of Administration

Mr. Wayne Simoneau, Commissioner
Department of Employee Relations

We have audited selected areas of the Minnesota Accounting and Procurement System (MAPS) and the Minnesota Statewide Employee Management System (SEMA4) for the period July 1, 1995, through March 31, 1996, as further explained in Chapter 1. Our audit primarily focused on the integrity of financial data in these new statewide computer systems. We emphasize that this has not been a complete audit of all components of the MAPS and SEMA4 systems. The Summary highlights our audit objectives and conclusions. We discuss these issues more fully in the individual chapters of this report.

We conducted our audit in accordance with generally accepted government auditing standards. Those standards require that we obtain an understanding of management controls relevant to the audit. The standards also require that we design the audit to provide reasonable assurance that the Departments of Finance, Administration, and Employee Relations complied with provisions of laws, regulations, contracts, and grants that are significant to the audit. Management of the Departments of Finance, Administration, and Employee Relations are responsible for establishing and maintaining the internal control structure and 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 Finance, Administration, and Employee Relations. This restriction is not intended to limit the distribution of this report, which was released as a public document on September 27, 1996.

James R. Nobles
Legislative Auditor

John Asmussen, CPA
Deputy Legislative Auditor

End of Fieldwork: June 21, 1996

Report Signed On: September 19, 1996

SUMMARY

State of Minnesota
Office of the Legislative Auditor
Centennial Office Building • St. Paul, MN 55155
612/296-4708

Minnesota Accounting and Procurement System
Minnesota Statewide Employee Management System
Selected Scope Financial Audit
For the Period July 1, 1995, through March 31, 1996

Public Release Date: September 27, 1996 No. 96-39

Background Information

In the late 1980's the Departments of Finance, Administration and Employee Relations determined that the state's primary financial systems needed updating. Beginning in 1991, the departments received legislative funding for the Statewide Systems Project, designed to replace the outdated accounting, procurement, and payroll systems and to develop a new human resource system. The new accounting and procurement systems are collectively referred to as the Minnesota Accounting and Procurement System (MAPS). The name of the new payroll/human resource system is the Minnesota Statewide Employee Management System, or SEMA4.

Selected Audit Areas and Conclusions

The focus of our first audit of the new systems was to identify and evaluate the controls that ensure data integrity. For each system, we reviewed security and access controls, reconciliations and other system control procedures, and subsystem interfaces. For MAPS, we also reviewed the conversion of prior year Statewide Accounting System (SWA) balances, updating of general ledger transactions, and appropriation control.

The administering departments found many technical problems with MAPS and SEMA4 after the conversion. Some of these problems made it difficult for state agencies to manage their financial activities. Many of these problems have already been corrected. The correction of the remaining problems will ultimately depend on the availability of resources.

Many users have more clearance to MAPS and its underlying data than they need to complete their job duties. Also, we found problems with some of the Department of Finance's security administration procedures. In addition, the department did not complete important accounting reconciliations, or adjust for known discrepancies, on a timely basis.

The Department of Finance implemented sufficient controls to ensure an accurate and complete transfer of subsystem data to MAPS and designed an effective process to convert SWA accounting records to MAPS. In addition, the department implemented sufficient controls to ensure that transactions are updating the appropriate accounts. However, we found that the Department of Finance does not verify the reasonableness of changes made to estimated receipt amounts that agencies have authority to spend.

Most SEMA4 users only have access to data pertaining to their own agency. However, a large number of users appear to have more clearance than they need to fulfill their job responsibilities. We also found some weaknesses in the Department of Employee Relation's security administration procedures. However, SEMA4 edits and system control reports are sufficient to detect material errors and irregularities in the financial data. In addition, the Departments of Employee Relations and Finance have sufficient controls to ensure an accurate and complete transfer of payroll expenditures to MAPS.

Contact the Financial Audit Division for additional information.
296-1235

Minnesota Accounting and Procurement System
Minnesota Statewide Employee Management System

Table of Contents

Audit Participation

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

John Asmussen, CPA	Deputy Legislative Auditor
Claudia Gudvangen, CPA	Senior Audit Manager
Christopher Buse, CPA, CISA	Director of Information System Audits
Beth Hammer, CPA, CISA	Audit Director
Brad White, CPA, CISA	Audit Director
Cecile Ferkul, CPA	Audit Director
Dave Poliseno, CPA, CISA	Team Leader
Carl Otto, CPA, CISA	Team Leader
Geniene Herrlich, CPA	Senior Auditor

Exit Conference

We discussed the issues in this report with the following staff from the Departments of Finance, Administration, and Employee Relations on September 5, 1996:

Department of Finance:

Laura King	Commissioner
Rosalie Greeman	Assistant Commissioner
Michael Ladd	Assistant Commissioner
Margaret Jenniges	Financial Reporting Director
Mary Bogie	Agency Support Director
Don Smith	Statewide Payroll Services Director

Department of Administration:

Kent Allin	Assistant Commissioner

Department of Employee Relations:

Chris Goodwill	Administrative Services Division Manager
Laurie Hansen	SEMA4 Project Team Leader

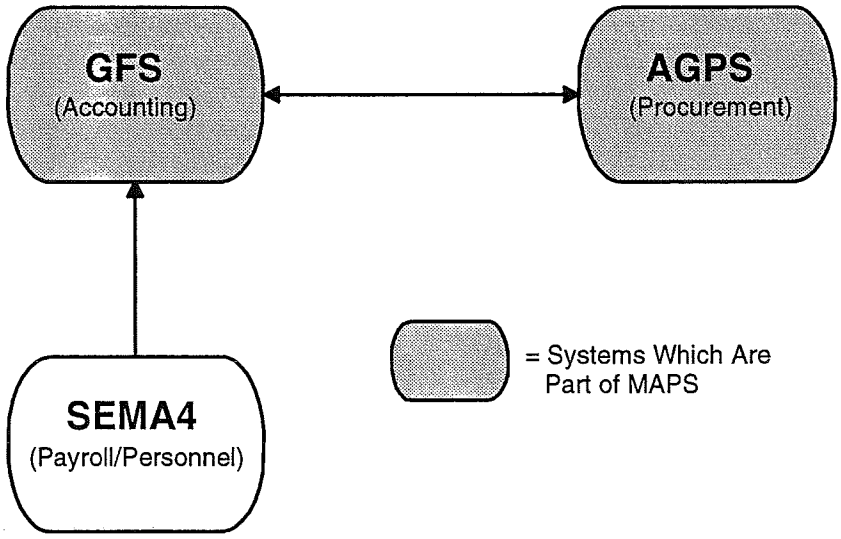
Chapter 1. Introduction

In the late 1980s, the Departments of Finance, Administration, and Employee Relations determined that the state's primary financial systems needed updating. In 1991, the Governor proposed a major information systems investment project to replace the outdated accounting, procurement, and payroll systems. The proposal also sought funding for a new human resource system, replacing previous manual records. The 1991 Legislature provided initial funding for the project, which ultimately became known as the Statewide Systems Project.

The mission of the Statewide Systems Project was to develop and maintain a comprehensive set of administrative systems. To fulfill its mission, the project team purchased three commercially available software packages and customized them to meet the specific needs of state agencies. Government Financial System (GFS) is the name of the new accounting system. The name of the new purchasing system is the Advanced Government Purchasing System (AGPS). Collectively, these two systems form an integrated group that is commonly referred to as the Minnesota Accounting and Procurement System (MAPS). The name of the new payroll/human resource system is the Minnesota Statewide Employee Management System, or SEMA4.

All three new systems interface to some extent. For example, AGPS and SEMA4 pass financial data to the GFS accounting system. This gives GFS the ability to provide perpetual accounting information that is all-inclusive. The GFS accounting and AGPS procurement systems work both interactively and independently. Users can perform some activities, such as encumbering funds and recording expenditures, in either AGPS or GFS. Other activities, such as budgeting or soliciting bids, can only occur in one system. Figure 1-1 illustrates the flow of data between GFS, AGPS, and SEMA4.

Figure 1-1
The Flow of Data Between the GFS, AGPS, and SEMA4 Systems



Source: Auditor prepared.

Minnesota Accounting and Procurement System
Minnesota Statewide Employee Management System

As of March 1996, there were approximately 3,800 MAPS and 1,700 SEMA4 users. State agencies began using MAPS in April 1995. With the exception of the Minnesota State College and University System (MnSCU), all state agencies converted to SEMA4 between July 1, 1995 and December 31, 1995. MnSCU developed its own personnel system and implemented an interface to use the SEMA4 payroll processing functions. The MnSCU interface with SEMA4 became operational in May 1996.

The Departments of Finance, Administration, and Employee Relations jointly administer and maintain the new statewide business systems. The Departments of Finance and Employee Relations have programming teams that are responsible for maintaining the computer software. They also have security functions that give users system access. In addition, staff from the three departments help users understand the new systems and resolve problems.

This is our first audit of the new statewide business systems. Therefore, our initial focus was to identify and evaluate the controls that ensure data integrity. For each system, we reviewed:

- Security and access controls;
- Reconciliations and other system control procedures; and
- Subsystem interface controls.

For MAPS, we also reviewed:

- The process used to convert the accounting records from the old Statewide Accounting System;
- How on-line transactions update general ledger accounts; and
- Controls that prevent agencies from exceeding their legal spending limits.

The administering departments found many technical problems with the MAPS and SEMA4 systems after the conversion. Major system development projects often experience these kinds of problems in the early stages of implementation. Some of these problems made it difficult for state agencies to manage their financial activities. For example, some standard MAPS financial reports were not accurate during the first half of fiscal year 1996. In general, however, the administering departments have an effective process to identify and prioritize the resolution of technical problems found after the conversion. The correction of all technical problems will ultimately depend on the availability of resources.

The Program Evaluation Division of our office is also reviewing MAPS and SEMA4 as part of its state computer systems development project. That project will focus, in part, on the decision-making process during development of the statewide systems. It will also consider whether the systems meet planned objectives and will identify benefits achieved. The Program Evaluation Division plans to issue its state computer systems development report in early 1997.

Chapter 2. Minnesota Accounting and Procurement System (MAPS)

Chapter Conclusions

The Department of Finance has implemented manual and computerized controls to ensure that MAPS data is accurate and complete. Our audit focused on the following five areas that impact the integrity of MAPS data:

***System Security** - The Department of Finance uses two different software packages to control access to MAPS and its underlying data. However, many users have more clearance than they need to complete their job duties. Also, we found problems with some security administration procedures.*

***System Integrity** - The Department of Finance performs several control procedures to ensure the accuracy and completeness of MAPS accounting records. However, it did not complete important accounting reconciliations on a timely basis. The department also did not promptly adjust the accounting records to correct discrepancies noted on system assurance reports.*

***Subsystem Interfaces** - The Department of Finance has implemented sufficient controls to ensure an accurate and complete transfer of subsystem data to MAPS.*

***Conversion from SWA to MAPS** - The Department of Finance designed an effective process to convert the accounting records from the old Statewide Accounting System (SWA) to MAPS.*

***Accounting Implications of Transactions** - The Department of Finance designed the MAPS system to ensure that transactions are updating the appropriate accounts.*

Finally, we found that, for most appropriations, the Department of Finance uses both manual and computerized controls to prevent agencies from exceeding legal spending limits. However, the Department of Finance does not verify the reasonableness of estimated receipt amounts that agencies have authority to spend.

The new Minnesota Accounting and Procurement System (MAPS) consists of two separate computerized applications. Government Financial System (GFS) is the name of the new accounting system. The name of the new purchasing system is the Advanced Government Purchasing System (AGPS). These two systems work both interactively and independently to account for most of the state's financial activities. Many trustee and local bank activities are still accounted for in separate subsystems.

The Statewide System Project team purchased the GFS and AGPS software from vendors. The team then customized these software packages to meet the unique needs of the state. For example, the team modified the GFS and AGPS software so that it would work in an "on-line, real-time" environment. This modification lets users enter financial transactions and immediately see the processed results.

Audit Scope and Objectives

This is our first audit of the new Minnesota Accounting and Procurement System. Therefore, our initial focus was to evaluate the controls which ensure the accuracy and completeness of financial data. However, we also reviewed controls over legal spending limits. The following is a summary of the key questions our work addresses:

- Was the Department of Finance controlling access to MAPS and its underlying financial data?
- Were MAPS reconciliations and system control reports sufficient to detect material errors and irregularities?
- Did the Department of Finance have sufficient controls over transactions entering MAPS through subsystem interfaces?
- Did the Department of Finance design and use an effective process to convert the accounting records from the old Statewide Accounting System to MAPS?
- Were MAPS on-line transactions updating the appropriate general ledger accounts?
- Did the Department of Finance have controls to prevent agencies from exceeding their legal spending limits?

To answer these questions, we interviewed Department of Finance employees and reviewed system documentation relating to each area. We also extracted and analyzed data from MAPS, including all general ledger and security transactions through March 31, 1996. The first five sections in this chapter discuss our work and conclusions reached on the accuracy and completeness of MAPS data. The last section discusses controls over appropriations.

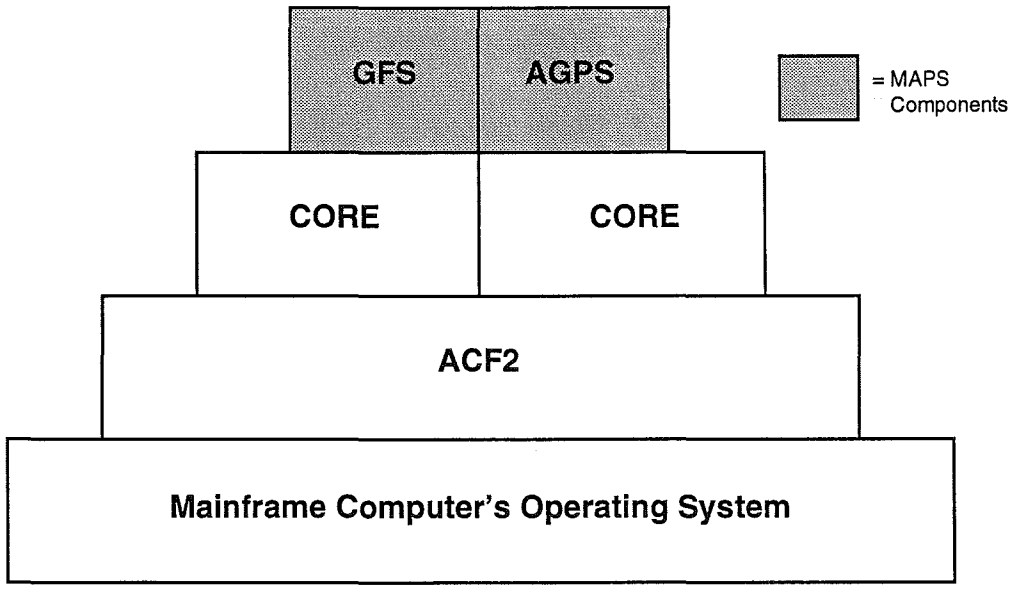
Section 1 -- Controlling Access to MAPS

MAPS financial data is a valuable asset to the State of Minnesota. To preserve the integrity of this data, it is important to have security policies and procedures which limit access. In general, users should only have the clearance necessary to perform their job responsibilities.

The Department of Finance uses several different software packages to secure access to MAPS and its underlying data. GFS and AGPS operate on two separate copies of a technical foundation called CORE. CORE is a computerized application that makes the development, maintenance,

and use of other applications more efficient. CORE also has a security module that the Department of Finance uses. GFS, AGPS, and CORE all run on the state's two central mainframe computers. A software package called ACF2 controls access to the mainframes. ACF2 acts as an extension of the computer's operating system and protects all data by default. Figure 2-1 shows the relationship between MAPS, CORE, and ACF2.

Figure 2-1
The Relationship Between MAPS, CORE, and ACF2



Source: Auditor prepared from discussions with Department of Finance employees.

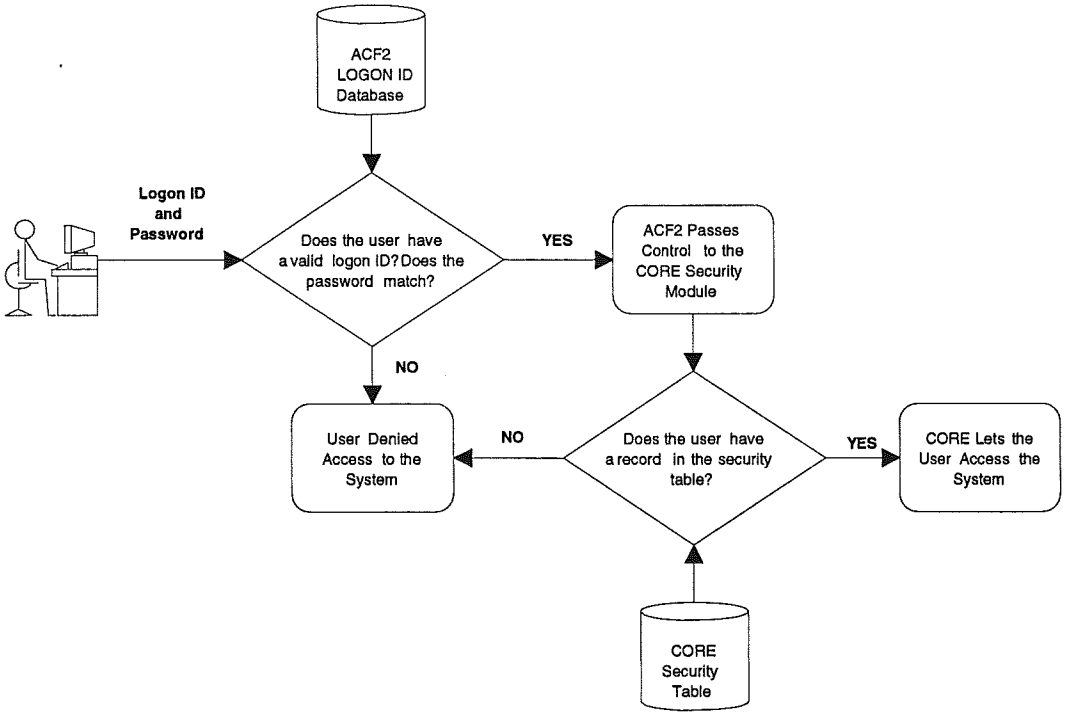
ACF2 uses unique logon IDs and passwords to control access to the mainframe computers. All users must enter their logon ID and password to access one of the state's central mainframes. ACF2 compares the user information to data stored in its logon ID database. The software denies access to users with unknown logon IDs or incorrect passwords. Once ACF2 authenticates a user, the CORE security module takes control. CORE checks its internal security table to determine if a mainframe user can access GFS or AGPS. Figure 2-2 illustrates how ACF2 and CORE control initial access to MAPS.

Once in GFS or AGPS, the CORE security module controls user actions. For example, GFS and AGPS have numerous data tables that users can access. CORE controls these access requests. CORE also controls access to GFS transactions. The CORE security module makes an allow or deny decision each time a user tries to access a data table or run a transaction.

ACF2 does far more than just secure initial access to the mainframe computers. It also controls access to mainframe files. All MAPS data resides in files that are stored on the state's two central mainframes. ACF2 protects these files from unauthorized destruction, disclosure, use, or

modification. The software will not allow access unless the security officer or the data owner explicitly authorizes that access. In essence, ACF2 protects against back door access attempts from outside GFS or AGPS. Without this protection, people with mainframe access could use various types of software to access and corrupt the state's financial data.

Figure 2-2
Gaining Initial Access to GFS and AGPS



Source: Auditor prepared.

Our specific audit objective was to determine if the Department of Finance was controlling access to MAPS and its underlying financial data. To fulfill this objective, we reviewed both the CORE security module and ACF2.

Based on these reviews, we conclude that the department needs to improve both its CORE and ACF2 security administration procedures. Also, many system users have more clearance than they need to fulfill their job responsibilities. The Department of Finance and user agencies each play a role in addressing these concerns.

CORE Security Administration

CORE uses an internal security table to control access to MAPS transactions and data. This security table serves two primary purposes.

- The table lists all standard security profiles. A standard security profile defines specific transactions available to users with that profile. It also defines the data tables that these users can access. Finally, a standard security profile describes the level of access authority. For example, one standard profile may only give users inquiry access to data while another may give them clearance to change that data.

- The table also lists the specific profile assigned to every authorized MAPS user. At the time of our audit, there were approximately 3,800 MAPS users.

The Department of Finance created approximately 100 standard security profiles. Each of these security profiles fits into one of 14 functional categories. The department defined functional categories to help agencies select profiles that match an individual employee's job responsibilities. For example, an agency choosing a profile for an accounts payable clerk would most likely review the various profile options in the "disbursement" category.

We identified several weaknesses in the department's CORE security administration procedures. We also found many system users who have more clearance than they need to perform their job responsibilities. Finding 1 discusses these issues. Finding 2 discusses our concerns with MAPS error overrides.

1. The Department of Finance has insufficient CORE security administration procedures.

The Department of Finance's CORE security administration procedures have several weaknesses. The department does not require specific agency employees to authorize system access request forms. The department also does not produce any reports to monitor security profiles or changes made to the CORE security table. Finally, the department does not scrutinize agency access requests for reasonableness.

Some agencies did not designate specific employees to serve as MAPS security liaisons. Agencies must complete an access request form for every GFS and AGPS user. These forms must be signed by the user's supervisor or another person designated by the agency. We feel that the department and user agencies could manage security more effectively if all agencies used designated security liaisons. This would help ensure that access requests are authorized by a person who is familiar with the various MAPS security profiles. It also would give the department a list of agency employees to contact to discuss security concerns.

The Department of Finance does not produce any CORE security reports. Without reports, agencies and the department cannot effectively manage security profiles assigned to individual users. Each agency, as well as the Department of Finance, should review security profiles on a continuing basis. The department also does not produce reports or log changes made to the CORE security table. The department did not begin saving electronic history files to support CORE security table changes until May 1996. Technical problems are currently limiting the usefulness of this data.

Finally, the Department of Finance does not scrutinize security profiles for reasonableness. Some security profiles in one functional category, called "Full Service," give users broad access

to MAPS data and transactions. The department designed these profiles primarily for agencies with small accounting staffs, where it is difficult to separate incompatible functions. However, as Table 2-1 illustrates, many medium and large agencies gave users incompatible full service profiles. We feel that this increases the risk of inappropriate financial activity.

Table 2-1
Percentage of Agency Users with Incompatible Full Service Security Profiles
As of May 1996

Agency	Total Agency Users	Users with Incompatible Profiles	% of Users with Incompatible Profiles
Supreme Court	9	9	100%
Attorney General	30	24	80%
IRRRB	19	15	79%
MnSCU	430	262	61%
Corrections	142	67	47%
Children, Families & Learning	28	12	43%
Human Services	314	129	41%
Employee Relations	22	9	41%
Economic Security	181	64	35%
Health	41	13	32%
Natural Resources	415	134	32%
Revenue	84	24	29%
Agriculture	62	15	24%
Administration	274	32	12%
Public Safety	270	52	19%
Transportation	524	69	13%
Trade and Economic Development	78	9	12%
Pollution Control	252	18	7%

Source: Auditor prepared from GFS Security Table (does not include all agencies).

We recognize that agencies are responsible for selecting the appropriate security profile for each of their users. However, as the system owner and security administrator, the Department of Finance needs to limit the use of incompatible profiles as much as possible. Furthermore, the Department of Finance should remind agencies of the risk associated with full service security profiles and suggest that mitigating controls may be necessary under some circumstances.

Recommendations

- *The Department of Finance should require state agencies to designate specific employees to serve as MAPS security liaisons.*

- *The Department of Finance should develop reports to monitor security profiles and changes to the CORE security table.*

- *The Department of Finance should develop guidelines to govern the use of incompatible full service security profiles.*

2. The Department of Finance does not control error overrides in MAPS.

The Department of Finance has not established adequate controls over error message overrides. MAPS has edits that prevent users from performing unallowable actions. When an edit interrupts transaction processing, the system displays an error message. However, most users have security profiles that give them the authority to override certain error messages. This authority is risky because it gives users the ability to process erroneous transactions.

Currently, all MAPS users who can process disbursements have the authority to override certain error messages. MAPS security officers gave users this authority because one edit program was not working properly. However, the security officers could not tell us if the edit program was ever corrected. They also did not know the specific error messages that users could override. Department managers were not aware that some users had override authority.

Recommendations

- *The Department of Finance should improve its understanding of override authority and evaluate its necessity.*

- *The Department of Finance should review transactions that were processed with override authority.*

ACF2 Security

ACF2 uses rules to control access to files stored on the mainframe. In general, users cannot access any data unless permitted by a rule. Two primary ACF2 rules control access to MAPS production data. Each of these rules contain detailed instructions that ACF2 uses to make allow or deny decisions.

ACF2 rule writing is a joint effort between user agencies and the Department of Administration's Intertechnologies Group (Intertech). Intertech security officers are responsible for writing the ACF2 rules which control access to MAPS data. However, an ACF2 security liaison within the Department of Finance communicates all security decisions to Intertech.

We identified several security concerns in the ACF2 rules that control access to MAPS. Of greatest significance, many employees have more clearance than they need to fulfill their job responsibilities. Finding 3 discusses our concerns with inappropriate security clearances. We also found conflicting, redundant, and dormant instructions within the ACF2 rules. Finding 3 discusses these rule management concerns as well.

3. The Department of Finance is not effectively managing the ACF2 security rules which control access to MAPS.

Internal controls over ACF2 security administration are weak for several reasons. The Department of Finance gave many users more clearance than they need to perform their job responsibilities. The department also is not performing important rule maintenance functions. These control weaknesses are exposing important and sensitive MAPS data to an unnecessary risk of loss or misuse.

Large groups of employees, both within and outside the department, have inappropriate ACF2 security clearances. Certain users have been given a broader level of access than is necessary. ACF2 can restrict access to individual users or groups of users. Therefore, rules that give security clearance to all mainframe users or entire agencies are rarely necessary or appropriate.

Computer programmers within the department have inappropriate security clearances. The department designed a special ACF2 security group for its computer programmers. This security group gives them complete and unfettered access to all MAPS data. Some computer consultants also have similar access rights. We do not feel that this level of clearance is necessary. Computer programmers typically work with test data in a special test environment. On some occasions, programmers need access to production data to perform maintenance functions. However, these occasions are rare and do not merit giving all programmers continuous and unrestricted access.

The department needs to start actively maintaining its ACF2 rules. We found many conflicting and dormant security instructions in the ACF2 rules that control access to MAPS. For example, one instruction gives every employee in a large state agency inquiry access to important files used by the Department of Finance's computer programmers. However, another instruction gives these same agency users the ability to both read and change this sensitive data. Dormant security instructions refer to those that cannot restrict or deny access to any mainframe user. It is important to delete dormant instructions because they can cause future security problems. New users who happen to meet the criteria specified in a dormant instruction can access the data the instruction was originally intended to protect. Many of these dormant instructions were originally written for consultants who are no longer working for the department. The department could avoid this problem in the future by adding effective dates to security rules. Instructions with effective dates automatically expire on a specific future date.

Recommendations

- *The Department of Finance should review existing ACF2 security rules to isolate and correct inappropriate security clearances and conflicting instructions.*
- *The Department of Finance should only give its computer programmers the clearance needed to complete their normal job duties.*
- *The Department of Finance should eliminate dormant instructions from its ACF2 security rules and use effective dates, when appropriate.*

Section 2 -- System Integrity

This section discusses procedures that the Department of Finance uses to monitor and ensure the integrity of MAPS financial data. For reporting purposes we classify these procedures in two broad categories - reconciliations and system assurance reports.

The department performs reconciliations and reviews system assurance reports to identify potential errors in the MAPS accounting records. Reconciliations compare MAPS financial information to sources external to the system. For example, the department compares the MAPS cash balance to the actual cash balance recorded in the State Treasurer's banking records. System assurance reports, on the other hand, analyze internal MAPS data to identify errors. For example, one system assurance report lists all transactions that do not balance. MAPS is a "double entry" accounting system, meaning that the debit and credit side of every transaction must balance.

Our specific objective was to determine if the MAPS reconciliations and system assurance reports were sufficient to detect material errors in the accounting records. To fulfill this objective, we analyzed several key MAPS reconciliations as well as the two daily system assurance reports.

MAPS Reconciliations and System Assurance Reports

The Department of Finance performs six primary MAPS reconciliations. These reconciliations help identify unrecorded and potentially erroneous transactions. Table 2-2 describes these reconciliations and their completion status as of May 1996.

We reviewed the cash, cash receipts, and unredeemed warrants reconciliations as part of this audit. These reconciliations identified many transactions that were not properly recorded in MAPS. For example, the cash and unredeemed warrants reconciliations identified a large number of unrecorded subsystem payments. However, the department did not detect or correct these errors for an extended period of time because it had not completed the reconciliations promptly. We noted this internal control weakness in a March 1996 audit report to the Department of Finance regarding the old Statewide Accounting System. In Finding 4, we indicate that this same problem exists with MAPS.

The department generates two daily system assurance reports; the Detailed General Ledger/Budget Consistency Report (SA1) and the Out-of-Sync Listing (SA3). The SA1 report lists all transactions with unbalanced debits and credits. The SA3 reports lists all instances where the detailed transactions are not properly updating the MAPS summary records.

Table 2- 2
Minnesota Accounting and Procurement System
Overview of the Six Primary MAPS Reconciliations Completed by Department of Finance
As of May 1996

Reconciliation	Purpose	Frequency	Status
Cash	Verifies the accuracy of the MAPS cash balance. This reconciliation compares the MAPS cash balance to external bank records prepared by the State Treasurer.	Monthly	The department had completed these reconciliations through December 1995.
Cash Receipts	Verifies the accuracy of the daily cash receipt transactions. This reconciliation compares the daily MAPS cash receipt transactions to external cash receipt records prepared by the State Treasurer.	Daily and monthly	The daily reconciliations are substantially complete. The department had not completed any monthly reconciliations.
Unredeemed Warrants	Verifies the accuracy of the "outstanding" warrants recorded on MAPS. Outstanding warrants are those that have been issued, but have not cleared the bank. This reconciliation compares the outstanding warrants recorded on MAPS to external records prepared by the State Treasurer.	Daily and monthly	The department was reconciling July 1995 unredeemed warrants.
Payroll	Verifies the accuracy of payroll expenditures recorded on MAPS. This reconciliation compares the total MAPS payroll expenditures to amounts recorded on SEMA4, the state's new payroll/personnel system.	Pay period basis	The department had reconciled three pay periods in December 1995 and January 1996.
Investments	Verifies the accuracy of investment balances recorded in MAPS. This reconciliation compares the investment balances in MAPS to external records prepared by the State Treasurer and the State Board of Investment.	Monthly	The department had completed this reconciliation through December 1995.
Loans and Advances	Verifies the accuracy of loan and advance balances recorded in MAPS. This reconciliation compares the MAPS loan and advance balances to information provided by various state agencies.	Monthly	The department had completed this reconciliation through July 1995

Source: Auditor prepared.

We reviewed the system assurance reports to determine if the department was investigating and correcting all exceptions. We also produced our own version of an SA1 report from the detailed general ledger transactions. Based on this work, we conclude that the system assurance reports are capturing exceptions. We also found evidence to indicate that the department was investigating the cause of each exception. However, as of May 1996, the department had not corrected the financial errors in the accounting records. Finding 4 discusses this issue in more detail.

4. The Department of Finance is not performing important control procedures in a timely manner.

The Department of Finance is not performing MAPS reconciliations timely. The department also is not promptly correcting errors identified by system assurance reports. As a result, errors in the MAPS accounting records can occur and remain undetected for extended periods.

Table 2-2 illustrates the delays in completing the six key MAPS reconciliations. As one example, the department did not complete the September 1995 cash reconciliation until April 1996. Inaccuracies in the MAPS accounting records may go undetected when reconciliations are not performed. In fact, the department's September 30, 1995 cash balance differed substantially from the State Treasurer's bank balance. Unrecorded transactions and errors accounted for a large portion of this difference.

The department also is not promptly correcting errors identified by system assurance reports. We reviewed the two system assurance reports and found MAPS financial errors of about $355,000. As of May 1996, the department had not corrected the accounting records.

Recommendations

- *The Department of Finance should perform reconciliations and review system assurance reports timely. The department should also promptly correct errors, when necessary.*

Section 3 -- Subsystem Interfaces

Many state agencies have their own computer systems that are independent of MAPS. In this section, we refer to these agency specific computer systems as "subsystems". Agencies need subsystems because MAPS does not support the unique data processing requirements of every program or business function. For example, the Minnesota State Retirement System has its own computer system that calculates and processes annuity payments for retirees. MAPS does not perform this function.

MAPS was designed to interact with agency subsystems. This interaction, called an interface, provides a mechanism to record subsystem transactions in the MAPS accounting records. There are two types of interfaces:

- **Interface Warrant Print (IWP)** - IWP accepts detailed transactions from agency subsystems and generates state warrants. IWP also records detailed or summarized accounting entries in MAPS. For example, the Department of Human Services uses IWP to pay numerous Medical Assistance providers. The IWP interface process summarizes these detailed payments into one or several accounting entries before updating MAPS.

- **Common Inbound Transaction Architecture (CITA)** - CITA also accepts detailed transactions from agency subsystems. However, the CITA interface process records the detailed transactions in MAPS. In essence, CITA facilitates and automates the process of accepting and entering financial transactions from agency subsystems. One of the main uses of the CITA interface is to transfer data from the state's payroll system (SEMA4) to MAPS.

Our specific audit objective was to determine if the department had sufficient controls over transactions entering MAPS through subsystem interfaces. To fulfill this objective, we analyzed both the IWP and CITA interface processes. We also analyzed the data that updated MAPS through these interfaces.

Subsystem Interface Controls

Most of the MAPS financial activity enters the system through subsystem interfaces. Therefore, it is important to control and secure these system entry points. Transactions entered directly in MAPS must face a series of edits. These edits help prevent erroneous transactions from updating the accounting records. Transactions entering MAPS through subsystem interfaces also should face the same or similar types of edits to protect the integrity of the state's financial data.

Table 2-3 compares and quantifies expenditure transactions processed through IWP and CITA to those entered directly in MAPS. Approximately 62 percent of the MAPS expenditure transactions enter the system through interfaces. These interface transactions account for approximately 70 percent of the state's total expenditures.

Table 2-3
MAPS Subsystem Interfaces
Comparison of Expenditure Input Methods
July 1, 1995 through March 31, 1996

Input Method	Total Number of Transactions	Percent of Total Number	Total Amount of Transactions	Percent of Total Amount
IWP	4,998	0.15%	$6,449,129,268	54.56%
CITA-Payroll	1,767,399	53.69%	$1,425,472,293	12.06%
CITA-Other Subsystems	259,164	7.87%	$362,195,020	3.06%
Direct MAPS Entries	1,260,142	38.28%	$3,582,768,747	30.31%
Totals	**3,291,703**	**100.00%**	**$11,819,565,328**	**100.00%**

Source: Auditor prepared from MAPS expenditure data.

Minnesota Accounting and Procurement System
Minnesota Statewide Employee Management System

In this section, we focus most of our discussion on the IWP interface process. Transactions entering MAPS through IWP account for approximately 55 percent of the state's total expenditures. However, IWP transactions account for less than one percent of the total transaction volume because they are summary entries. Most of the CITA transactions are the result of the interface with the state's payroll system. We discuss controls over this CITA interface process in Chapter 3.

The main features of the IWP process are that it produces warrants centrally and enters summary accounting data on MAPS. Agencies that use IWP generally have a high volume of transactions that are very similar in nature. Table 2-4 shows the agencies that use IWP, the type of payments made, and the financial activity.

Table 2-4
Materiality of IWP Interfaces
July 1, 1995 through March 31, 1996

State Agency	Type of Payments	Amount
Children, Families & Learning	School Aids	$2,464,658,654
Human Services	Medical Benefits	2,336,361,217
Revenue	Local Government Aids	872,515,095
Transportation	State Transportation Aids	277,133,118
Teachers Retirement Association	Annuity Payments and Refunds	276,668,202
MN State Retirement System	Annuity Payments and Refunds	152,861,833
Labor & Industry	Special Workers Compensation	56,041,740
Employee Relations	Workers Compensation	7,098,425
Higher Education Services Office	Scholarships & Grants	5,790,984
Total IWP Payments		**$6,449,129,268**

Source: Auditor prepared from MAPS expenditure data.

Each subsystem submits detailed transactions to initiate IWP processing. These transactions must pass a series of validating edits before actual acceptance into IWP. The edits verify that the data is in the required format and that the detailed record count agrees with a control total on the file. The edits also verify that all transactions provide the required MAPS accounting information. The IWP process then prints warrants and records summary accounting entries in MAPS. The IWP process also creates a file that the State Treasurers Office uses to update its unredeemed warrant records. All IWP warrants clear through the State Treasurer's Office using the same process as regular state warrants.

The key controls in this process are:

- **IWP processing edits** - The initial editing of IWP is to verify the content of the subsystem data and ensure that the data is complete and valid prior to processing. This eliminates the risk that unauthorized or incorrect subsystem data could compromise the integrity of MAPS data through the IWP process.

- **Reconciliations of Cash and Unredeemed Warrants** - These reconciliations, which we discussed in Section 2, ensure that the MAPS financial information agrees with the actual transactions processed through the State Treasurer's Office.

- **Verification of MAPS entries to subsystem data** - State agencies originating IWP processing of subsystem transactions should be verifying that the summary MAPS entries agree with the subsystem data they submitted for processing.

For the IWP process, we conclude that the design of controls was sufficient to ensure an accurate and complete transfer of the subsystem financial data to MAPS. However, these controls rely on external reconciliations of cash and unredeemed warrants. As discussed in Finding 4, the Department of Finance did not perform these key control procedures in a timely manner.

Section 4 -- Conversion from SWA to MAPS

During the first few months of fiscal year 1996, the state was simultaneously operating both the old Statewide Accounting System (SWA) and MAPS. State agencies began processing fiscal year 1996 transactions in MAPS in April 1995. Agencies continued to process fiscal year 1995 transactions in SWA until the Department of Finance closed the books on October 13, 1995. After this date, the department transferred the remaining account balances to MAPS.

Our specific objective for this section was to determine whether the Department of Finance had sufficient procedures to ensure that the beginning account balances on MAPS were accurate. We focused our review on the process used to convert SWA account balances to MAPS.

The Department of Finance separated the conversion process into four areas and established procedures for each area. These four areas included:

- **Balance Sheet Accounts** - The department moved cash into MAPS as it converted fiscal year 1995 appropriation accounts. The department then used the SWA Post Closing Trial Balance Report to transfer all remaining balance sheet account balances to MAPS.

- **Encumbrances** - An encumbrance is a reservation of an agency's budget for a specific purchase. After the fiscal year 1995 close, the Department of Finance worked with state agencies to identify all valid SWA encumbrances. The department then transferred the lessor of the encumbrance amount or the unliquidated cash amount to MAPS.

- **Fiscal Year 1995 Carryover to 1996** - This conversion process involved moving balances from fiscal year 95 to 96 for agencies with legislative authority to carry forward funds. The department identified and moved amounts based on SWA report balances.

- **Multi-Year Project Appropriation Transfers** - These balances pertain to projects where the legislature did not limit spending to specific fiscal years. Agencies have the authority to carry forward these funds until the completion of the project. The department determined the remaining balances for each project and created a new appropriation record in MAPS to account for the funds.

Based on our review, we conclude that the department designed and used an effective process to convert the accounting records from SWA to MAPS.

Section 5 -- Accounting Implications of Transactions

MAPS updates its general ledger accounting records when users enter transactions. There are many different types of MAPS transactions, most of which perform a specific double entry accounting function. For example, a cash receipt transaction records the receipt of cash as well as an increase to revenue.

Our specific objective was to determine if the Department of Finance designed the system to ensure that MAPS transactions were updating the appropriate general ledger accounts. To fulfill this objective, we interviewed accounting personnel from the Department of Finance and analyzed the detailed general ledger transactions recorded in MAPS during March 1996.

We focused our review on the following three transaction types:

- **Cash receipt** - This transaction type records the receipt of cash. Agencies use it to record collections against outstanding accounts receivable, cash basis revenue, and non-revenue-related receipts such as expenditure refunds.

- **Payment voucher** - This transaction type authorizes the spending of funds and initiates automated warrant writing procedures.

- **Journal voucher** - This transaction records accounting events that users cannot record with any other MAPS transaction type. The Department of Finance limits the use of journal vouchers.

For each of these transactions, we reviewed the specific general ledger accounts that were updated. Based on our review, we conclude that MAPS transactions are updating the appropriate general ledger accounts.

Section 6 -- Appropriation Control

Minnesota law requires the Department of Finance to ensure that agencies have sufficient spending authority before incurring obligations. MAPS provides budgetary accounting features to prevent agencies from exceeding their legal spending authority. These features include appropriation and allotment records and expense budgets.

An appropriation is a dollar amount allocated by law or statute for a specific purpose. MAPS appropriation records help the Department of Finance enforce these legal spending limits. In general, MAPS will not let a user exceed the legal spending authority established by an appropriation record.

Minnesota Accounting and Procurement System
Minnesota Statewide Employee Management System

Our specific audit objective was to determine if the Department of Finance had controls to prevent agencies from exceeding their legal spending limits. State agency employees and the Department of Finance complete a number of steps and make important decisions when creating MAPS appropriation records. This section discusses these steps and decisions, as well as the risks associated with establishing appropriation records.

In our opinion, the department has controls to prevent agencies from exceeding their legal spending limits. However, the processes used to record and transfer appropriation records in MAPS have some weaknesses.

Creating MAPS Appropriation Records

Agencies cannot obligate or spend funds without an appropriation record in MAPS. The Department of Finance is responsible for entering appropriation records in the system. This process begins when an agency submits an Appropriation Entry Form. The Department of Finance reviews these forms and the underlying legal citations to verify the accuracy of important MAPS appropriation codes. The department also verifies that the new appropriation record will not provide the agency with an opportunity to exceed its legal spending authority.

MAPS uses a number of factors to calculate the legal spending limit for an appropriation record. The appropriation amount specified in law is the primary factor. However, the spending limit calculation becomes more complex when the legislature gives agencies the authority to carryover prior year funds or to spend receipts. MAPS uses appropriation type and budget authority codes to identify these special circumstances. Agencies are responsible for determining the proper codes to list on the Appropriation Entry Form. The Department of Finance also reviews the specific legal citations to verify the accuracy of these codes. Table 2-5 illustrates the total spending authority for all appropriation records as of March 1996.

Table 2-5
Minnesota Accounting and Procurement System
Total Spending Authority for All Appropriation Accounts

Source of Funds	Fiscal Year 1996 Totals
Direct Appropriations	$13,705,558,487
Net Carryover from prior fiscal years	1,494,115,788
Cancel/Reverted	(1,957,463)
Anticipated Dedicated Receipts	5,649,831,420
Total Spending Authority (Note 1)	**$20,847,548,232**

Note 1: This total includes all anticipated dedicated receipts. In some cases, agencies may only have authority to spend actual receipts which may differ from anticipated. In addition, legal citations may contain a ceiling that limits spending to a specified amount.

Source: Fiscal year 1996 appropriation table (as of March 1996).

MAPS uses appropriation type codes to determine if an agency can carryover funds to the next fiscal year. Table 2-6 describes the various appropriation type codes. The table also lists the number of appropriation records and the total spending authority for each code. Code 4, which refers to special appropriations that always carry forward, has the largest spending authority.

Table 2-6
Minnesota Accounting and Procurement System
Valid Appropriation Type Codes

Code	Code Name	Year End Result	# of FY 96 Records	Spending Authority
01	Regular	Cancels at year end	472	$ 4,175,123,118
02	Continuing	Spans multiple years	106	3,243,672,121
03	Supplemental	New appropriation beginning during the year	1	0
04	Special	Always carries forward	3,162	7,674,972,577
05	Biennial	Carries forward first year, cancels the second year of the biennium	1,050	2,714,084,752
06	Open	Allows whatever spending is necessary to fund program	220	3,039,695,664
		Total	**5,011**	**$20,847,548,232**

Source: Department of Finance policies and procedures and the March 1996 appropriation table.

MAPS uses budget authority codes to determine how receipts impact an appropriation's spending authority. Table 2-7 lists the six budget authority codes and describes how each code impacts spending authority calculations. The table also displays the number of fiscal year 1996 appropriation records with each code and the total spending authority.

Table 2-7
Minnesota Accounting and Procurement System
Valid Budget Authority Codes

Code	Spending Authority Calculation	# of FY 96 Records	Spending Authority
N	No receipts	1,863	$10,603,426,191
A	Actual receipts	44	21,079,569
E	Estimated receipts	4	12,940,630
G	Greater of actual or estimated receipts	347	3,504,827,646
L	Lessor of actual or estimated receipts	0	0
O	Encumber estimated/spend actual receipts	2,753	6,705,274,196
	Total	**5,011**	**$20,847,548,232**

Source: Department of Finance policies and procedures and the March 1996 appropriation table.

Selecting the proper budget authority code is an extremely important decision. Some budget authority codes, such as "E" and "G", give agencies the ability to spend estimated receipts. The Department of Finance does not monitor the estimated receipt transactions entered by agencies. Finding 5 discusses our concerns with controls over these estimated receipt transactions.

Appropriation Transfers

On some occasions, agencies need to transfer funds between appropriations. The Department of Finance has a policy that requires agencies to complete an anticipated appropriation transfer transaction before completing an actual transfer. MAPS will not process these anticipated appropriation transfers until they have been approved by the Department of Finance.

The transfer process has an inherent weakness, however. MAPS will let an agency enter an actual appropriation transfer without first entering an anticipated transfer. As a result, agencies are able to bypass the Department of Finance's approval process. To remedy this weakness, the department produces a monthly exception report that identifies actual appropriation transfers without corresponding anticipated transfers. We found evidence indicating that the department was investigating all exceptions on this report and monitoring agency resolutions. However, because the report is only run monthly, there is risk that an agency could incur obligations based on an inappropriate transfer.

5. The Department of Finance does not verify the reasonableness of estimated receipts amounts that agencies have authority to spend.

The Department of Finance has not established specific procedures to monitor some high risk estimated receipt transactions. Agencies enter estimated receipts in MAPS. As Table 2-7 shows, two budget authority codes allow agencies to spend these estimated receipts. The Department of Finance requires agencies to obtain special approval to use these two codes. The department also reviews the initial revenue budgets established by agencies. However, the department does not have specific procedures in place to review or monitor changes made to these revenue budgets. As a result, there is a risk that agencies will incur obligations based on inflated receipt estimates.

Recommendation

- *The Department of Finance should monitor estimated receipt transactions when agencies have the authority to spend these receipts.*

Chapter 3. State Employee Management System (SEMA4)

Chapter Conclusions

The Department of Employee Relations and the Department of Finance have implemented manual and computerized controls to ensure that SEMA4 data is accurate and complete. Our audit focused on three areas that impact the integrity of SEMA4 data, including:

System Security - The SEMA4 system has an internal security module that the Department of Employee Relations and the Department of Finance use to control access to the system and its underlying financial data. Most SEMA4 users only have access to data pertaining to their own agency. However, a large number of these users appear to have more clearance than they need to fulfill their job responsibilities. We also found some security administration procedure weaknesses.

SEMA4 Data Integrity - SEMA4 edits and system control reports are sufficient to detect material errors and irregularities in the financial data. SEMA4 edits help identify potentially erroneous data at its point of origin. Standard reports are sufficient to identify material errors or irregularities in the SEMA4 data, should they occur.

Subsystem Interfaces - The Department of Employee Relations and the Department of Finance have sufficient controls to ensure an accurate and complete transfer of payroll expenditures to MAPS. However, as discussed in Chapter 2, important payroll reconciliations were not performed timely.

The state of Minnesota implemented an integrated human resource and payroll system on July 1, 1995. The name of this new system is the Statewide Employee Management System (SEMA4). All state agencies are now using SEMA4. However, the Minnesota State College and University System (MnSCU) developed its own human resource system to meet its unique personnel needs. MnSCU and the Departments of Employee Relations and Finance designed an interface for this human resource system. This gives MnSCU the ability to use the SEMA4 payroll processing capabilities. This interface became operational in May 1996.

SEMA4 performs both human resource and payroll processing functions. The state's previous system, on the other hand, was primarily a payroll system. Major functions of the new SEMA4 system include:

- Processing the biweekly payroll;

- Managing positions;
- Controlling employee business expenses;
- Allocating payroll expenditures to various funding sources; and
- Managing employee personnel and training information.

Agency personnel officers use SEMA4 to create employee records and assign compensation levels. In most instances, negotiated bargaining agreements govern these personnel transactions. Agency personnel officers also may establish a separate position for each employee and determine the appropriate funding source or sources. Agency payroll officers enter employees' time, leave, and business expenses in the system. After payroll processing, a system interface transfers expenditure data to the Minnesota Accounting and Procurement System (MAPS).

Audit Objectives and Scope

The focus of our first audit of the new Statewide Employee Management System was to evaluate the controls which ensure the accuracy and completeness of financial data. The following is a summary of the key questions our work addresses:

- Were the Department of Employee Relations and the Department of Finance controlling access to SEMA4 and its underlying financial data?

- Were SEMA4 edits and system control reports sufficient to detect material errors and irregularities?

- Did the Departments of Employee Relations and Finance have sufficient controls to ensure that all relevant payroll transactions update the MAPS accounting records?

To answer these questions, we interviewed employees from the Department of Employee Relations and the Department of Finance. We also reviewed system documentation relating to each area. The following three sections discuss the results of our work.

Section 1 -- Controlling Access to SEMA4

It is important to control access to SEMA4 because the system stores sensitive payroll and personnel data. Financial data which must be protected includes hours worked, leave balances, pay rates, and deductions. Sensitive human resource data includes employee personnel information, absence histories, disciplinary actions, grievances, and salary garnishments. In general, SEMA4 users should only have the clearance necessary to perform their job responsibilities.

Several different software packages control access to SEMA4 and its data. The SEMA4 system was developed from a commercial software package called Peoplesoft. The Departments of Employee Relations and Finance use the internal security module that came with Peoplesoft to control access to SEMA4. SEMA4 stores payroll and personnel data in a database management system called DB2. DB2 also performs some security and data integrity functions. The DB2

database resides on the state's two central mainframe computers. As discussed in Chapter 2, a software package called ACF2 controls access to the mainframes.

ACF2 uses unique logon IDs and passwords to control access to the mainframe computers. All users must enter their logon ID and password to access one of the state's central mainframes. ACF2 compares the user information to data stored in its logon ID database. The software denies access to users with unknown logon IDs or incorrect passwords. Once ACF2 authenticates a user, the SEMA4 internal security module takes control. SEMA4 checks its internal security table to determine if a mainframe user can access the system.

Once in SEMA4, the internal security module controls all user actions. For example, the system has numerous data tables that users can access. The internal security module controls these access requests. The security module makes an allow or deny decision each time a user tries to access a data table or run a transaction.

Our audit objective was to determine if the Departments of Employee Relations and Finance were controlling access to SEMA4 and its underlying financial data. To fulfill this objective, we gained an understanding of the SEMA4 internal security module and the process used to assign security profiles to agency users. We also analyzed the SEMA4 security tables to review the specific profile or profiles assigned to each system user. We did not, however, review the ACF2 or DB2 security structure as part of this audit.

We conclude that the Departments of Employee Relations and Finance are using the Peoplesoft security capabilities to control access to SEMA4 and its underlying financial data. Most SEMA4 users only have access to data pertaining to their own agency. However, a large number of these users have more clearance than they need to fulfill their job responsibilities. Finding 6 discusses our concerns with inappropriate security clearances. Finding 6 also discusses some weaknesses in the security administration procedures.

SEMA4 Internal Security Module

User agencies and the Departments of Employee Relations and Finance are jointly responsible for SEMA4 security administration. The Department of Employee Relations maintains and updates data in the SEMA4 security module. This data includes the specific security profile or profiles assigned to each authorized user. Agencies are responsible for reviewing the job responsibilities of each user and selecting the appropriate security profile or profiles. The Department of Employee Relations supplied each agency with a description of every standard human resource and payroll profile.

6. The Departments of Employee Relations and Finance have several weaknesses in their SEMA4 security administration procedures.

The Departments of Employee Relations and Finance do not distribute security reports to agencies on a regular basis or log changes made to security tables. As a result, it is difficult to monitor security profiles and transactions on a regular basis. The departments also do not scrutinize agency access requests for reasonableness. We reviewed the SEMA4 security tables

and found many users that appear to have more clearance than they need to perform their job duties. Specifically, many users have the clearance to update both payroll and personnel records. This level of clearance increases the risk of inappropriate transactions.

The Departments of Employee Relations and Finance have not developed a structured security reporting and verification process. Without standard reports, agencies and the departments cannot effectively manage security profiles. Each agency, as well as the Departments of Employee Relations and Finance, should review security profiles on a continuing basis. The departments also do not maintain an electronic history file of changes made to the SEMA4 security tables. The departments update records in the SEMA4 internal security module. However, the system does not save copies of the records that were changed. Without this data, the departments cannot ensure that only authorized changes were made to the security tables.

Finally, the Departments of Employee Relations and Finance do not scrutinize agency access requests for reasonableness. The departments created separate payroll and human resource profiles so that agencies could separate incompatible duties. However, many agencies gave their users security profiles that allow them to enter both payroll and human resource transactions. The departments did not question the appropriateness of these access requests. We analyzed the June 1996 security table and found that over 27 percent of the system users could enter both payroll and human resource transactions. Table 3-1 illustrates these results by agency.

Table 3-1
State Employee Management System
Agency Users Who Can Enter Both Payroll and Human Resource Transactions
As of June 1996

Agency	Total Agency Users	Users with Incompatible Profiles	% of Total Agency Users
Transportation	259	128	49.4%
Economic Security	50	22	44.0%
Administration	39	13	33.3%
Natural Resources	150	44	29.3%
Human Services	203	59	29.1%
Corrections	138	36	26.1%
Revenue	72	13	18.1%
Finance	94	2	2.1%
Public Safety	105	2	1.9%
Employee Relations	146	1	0.7%
Other Agencies	421	145	34.4%
Totals	**1,677**	**465**	**27.7%**

Source: Auditor analysis of SEMA4 security tables as of June 1996.

We recognize that agencies are responsible for selecting the appropriate security profiles for each of their users. We also realize that in some instances agencies may need to grant broad access to employees when their staff size is limited. However, as the system owner and security

administrator, the Departments of Employee Relations and Finance need to limit the use of powerful profiles as much as possible. Furthermore, the departments should warn agencies about the risks associated with allowing employees to have incompatible profiles.

Recommendations

- *The Departments of Employee Relations and Finance should formalize their security reporting and verification procedures.*
- *The Departments of Employee Relations and Finance should log changes made to SEMA4 security tables.*
- *The Departments of Employee Relations and Finance should develop guidelines to govern the use of incompatible payroll and human resource security profiles.*

Section 2 -- SEMA4 Data Integrity Controls

SEMA4 data integrity responsibilities are shared jointly by user agencies, the Department of Employee Relations, and the Department of Finance. SEMA4 employs both preventive and detective controls to maintain data integrity. Preventive controls try to identify inaccurate or incomplete data before it updates the system. Error messages are a common type of preventive control used by SEMA4. Detective controls, on the other hand, try to identify inaccurate or incomplete data after it has been processed. Exception reports are one mechanism that SEMA4 uses to highlight data that may be inaccurate or incomplete.

Our audit objective was to determine if SEMA4 edits and system control reports were sufficient to detect material errors and irregularities. To fulfill this objective, we reviewed the preventive edits used to identify potential data errors at their point of origin. We also reviewed system output and exception reports. Based on this work, we conclude that the system effectively edits data at its point of origin. We also feel that the various SEMA4 reports are sufficient to detect material errors or irregularities, should they occur.

Preventive and Detective Controls

The system displays warning or error messages when users enter data that is unreasonable or may be inappropriate. Warning messages alert users to possible data errors, but do not require further action. For example, SEMA4 displays a warning message if an employee's total hours exceeds 80. Error messages, on the other hand, identify data errors that must be corrected before processing can continue. For example, the system will display an error message if a user enters a pay rate that is outside a position's acceptable range. Processing cannot continue until the user enters a rate within the acceptable range.

A wide variety of standard and ad hoc reports help user agencies, the Department of Employee Relations, and the Department of Finance detect errors in SEMA4 data. The Departments of Finance and Employee Relations produce some reports for central oversight of the system. For

example, the Department of Finance is in the process of developing a report that identifies employees receiving gross pay over a certain significant dollar level. Other reports are designed for use by both user agencies and the Departments of Finance and Employee Relations. For example, the Payroll Register and the Payroll Posting Audit Trail help agencies confirm the accuracy and completeness of biweekly payroll transactions.

Section 3 -- The SEMA4 Interface to MAPS

Payroll needs to be promptly recorded in the MAPS accounting records because it is one of state's most significant expenditures. The Department of Finance uses a special interface process, called the Common Inbound Transaction Architecture (CITA), to pass payroll expenditures to MAPS. This section discusses controls over the CITA interface process for SEMA4 payroll transactions. Chapter 2 also provides a general overview of the CITA interface process.

Our audit objective was to determine if the Departments of Finance and Employee Relations have controls to ensure that all relevant SEMA4 payroll transactions update the MAPS accounting records. To fulfill this objective, we interviewed employees from the Departments of Finance and Employee Relations to gain an understanding of CITA and the procedures used to reconcile payroll expenditures between SEMA4 and MAPS. We also reviewed reconciliation documentation, to the extent available.

Transferring and Reconciling SEMA4 Payroll Expenditures

Every pay period, summarized SEMA4 payroll transactions pass through the CITA interface to MAPS. The Department of Finance performs a key reconciliation to verify the accuracy and completeness of this interface process. Specifically, for each pay period, the department reconciles the total payroll expenditures that updated MAPS to amounts recorded on SEMA4.

It took the Departments of Finance a considerable amount of time to develop this reconciliation. Therefore, the fiscal year 1996 reconciliations were not completed timely. In fact, we reviewed the reconciliations as of April 1996 and found only three pay periods that were complete. Finding 4, in Chapter 2, discusses our concerns with the timeliness of system reconciliations in more detail. The payroll reconciliations identified immaterial differences between the MAPS and SEMA4 expenditures. The Department of Finance is currently researching the cause of these differences and plans to perform timely reconciliations in the future.

State of Minnesota
Department of Finance

400 Centennial Building
658 Cedar Street
St. Paul, Minnesota 55155
Voice: (612) 296-5900
TTY/TDD: (612) 297-5353 or
Greater Minnesota 800-627-3529
and ask for 296-5900
Fax: (612) 296-8685

September 17, 1996

Mr. James Nobles
Legislative Auditor
100 Centennial Office Building
658 Cedar Street
St. Paul, MN 55155

Dear Mr. Nobles:

The purpose of this letter is to respond on behalf of the Departments of Finance and Employee Relations to the recent audit performed by the Office of the Legislative Auditor concerning the Minnesota Accounting and Procurement System (MAPS) and the Statewide Employee Management System (SEMA4) .

Your office recently completed a selected scope audit for the period July 1, 1995 to March 31, 1996 intended to "identify and evaluate the controls that ensure data integrity." This audit represents the first review of the state's new administrative systems since they were put into production in April 1995. Your staff is to be commended for identification of the key control and data integrity elements.

We have reviewed your findings with your staff and are in substantial agreement with the comments and resultant recommendations. Your audit was divided into nine major areas with comments and/or recommendations within each area. Consequently, our remarks are grouped into sections in order to aid understanding of the issues.

Five of the nine areas of the MAPS and SEMA4 review had no adverse findings or recommendations for improvement. Your staff found that certain access controls, data assurances and data integrity had been appropriately designed, implemented and monitored. We were gratified that our efforts in these areas succeeded in safeguarding the state's accounting and personnel information. The areas with no findings/recommendations for improvement were:

Chapter 2 (MAPS) - Subsystem interfaces
Conversion from SWA to MAPS
Accounting implementation of transactions

Chapter 3 (SEMA4) - Data integrity controls
Interfaces to MAPS

The report also contains five recommendations which the Department of Finance has already implemented. Listed below by chapter number is a brief description of the status of these recommendations:

CHAPTER 2 (MAPS) - The Department of Finance...

System Security - ... should review existing ACF2 security rules to isolate and correct inappropriate security clearances and conflicting instructions.

... should eliminate dormant instructions from its ACF2 security rules and use effective dates, when appropriate.

Response: *All ACF2 rules have been reviewed and instances of dormant or conflicting instructions or clearances have been eliminated. Staff from InterTech, Finance and the Auditor's Office will continue examination of ACF2 administration.*

... should improve its understanding of override authority and evaluate its necessity.

Response: *The only currently allowable "override-able error" is in the project billing module; this error does not impact cash transactions, it is related only to the allocation of costs. However, the entire policy has been reviewed as a result of this finding. All override authority has been reviewed for necessity.*

... should only give its computer programmers the clearance needed to complete their normal job duties.

Response: *A complete review of current security clearances for programmers is underway. Policies are being revised for future security clearance applications which will assure that only appropriate clearance is granted.*

System Integrity - ... should perform reconciliations and review system assurances reports timely. The department should also promptly correct errors, when necessary.

Response: *The department has made substantial progress in this area since the completion of the audit field work by OLA staff. The FY1996 financial reconciliations are now up to date. Five of the six MAPS reconciliations are current as of July records. The sixth area is current as of June 1996. All adjustments to MAPS as a result of these reconciliations*

will be completed before the end of September 1996. Errors identified by system assurance reports have been corrected in the accounting records.

The report also contained eight recommendations which we have begun to implement. Outlined below are the steps taken and estimated timetable to reach full implementation.

CHAPTER 2 (MAPS) - The Department of Finance...

System Security - ... should require state agencies to designate specific employees to serve as MAPS security liaisons.

Response: *Currently, twelve predominantly large state agencies have a designated liaison. We will develop a policy requiring all agencies to designate a security liaison as an alternate process addressing the control concerns.*

... should develop guidelines to govern the use of incompatible full service security profiles.

Response: *We will develop a policy for assigning security profiles for incompatible functions. Because there is often a legitimate business need for these profiles, especially in small agencies, we will include an explanation of the risks and the need for alternative controls.*

... should develop reports to monitor security profiles and changes to the CORE security table.

Response: *The existing CORE software does not produce the recommended report. Department resources have been directed toward higher priority report development. Security clearances have been reviewed and agency verification will be requested. We will continue efforts to identify an alternative solution.*

... should review transactions that were processed with override authority.

Response: *There is no evidence that improper payment transactions occurred, or that this feature otherwise compromised the basic financial records. Processes are being developed to prevent and/or detect future inappropriate override of system errors. This will include removing override authority from users' security profiles, except for those few identified by Finance and agencies as necessary. Also, we will remove all unused override-able errors and will monitor to verify that no new override-able errors have been created.*

Accounting implications of transactions - ... should monitor estimated receipt transactions when agencies have the authority to spend these receipts.

Response: *Policies and procedures will be developed as a part of FY98 budget implementation which will improve the monitoring of estimated receipts. Staff will increase regular review of revenue budget changes during FY97.*

CHAPTER 3 (SEMA4) - The Department of Employee Relations...

System Security - ... and Finance should formalize their security reporting and verification procedures.

... should develop guidelines to govern the use of incompatible payroll and human resources security profiles.

Response: *Reports have been designed and agency sign-off will be required. Additional security training will be designed and delivered. Agencies will be reminded of the existing profile policies, and considerations and consequences of incomparability risks will be reiterated.*

... and Finance should log changes made to SEMA4 security tables.

Response: *SEMA4 is not able to electronically support effective-date tracking of security profile changes. We have identified and will develop alternative reports to monitor transactions by agencies and central users in DOF and DOER.*

Commissioner Wayne Simoneau and I have directed that all pending recommendations be resolved by December 1, 1996. I have placed Rosalie Greeman, Assistant Commissioner for Accounting Services in the Department of Finance, in charge of assuring satisfaction concerning MAPS recommendations. Ms. Chris Goodwill, Executive Officer from the Department of Employee Relations, is responsible for SEMA4 related issues.

Warmest regards,

Laura M. King
Commissioner