Department of Administration

Financial Audit
For the Fiscal Year Ended June 30, 1995

February 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

96-7

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. Elaine Hansen, Commissioner
Department of Administration

We have audited selected aspects of the Department of Administration for the fiscal year ended June 30, 1995, as further explained in Chapter 1. The work conducted in the department is part of our Statewide Audit of the State of Minnesota's fiscal year 1995 financial statements. The Comprehensive Annual Financial Report for the year ended June 30, 1995 includes our opinion thereon dated December 1, 1995. This was not a complete audit of all financial activities of the Department of Administration. The following Summary highlights the audit objectives and conclusions. We discuss our concerns 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. These standards also require that we design the audit to provide reasonable assurance that the Department of Administration complied with provisions of laws and regulations that are significant to the audit. The management of the Department of Administration is 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 Department of Administration. This restriction is not intended to limit the distribution of this report, which was released as a public document on February 9, 1996.

James R. Nobles
Legislative Auditor

John Asmussen, CPA
Deputy Legislative Auditor

End of Fieldwork: December 1, 1995

Report Signed On: February 2, 1996

SUMMARY

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

Department of Administration

Financial Audit
For the Fiscal Year Ended June 30, 1995

Public Release Date: February 9, 1996 No. 96-7

Background

The mission of the Department of Administration is to provide business management and administrative services that improve the productivity and quality of Minnesota government. The department services both state and local government agencies. Its programmatic areas include Operations Management, the Intertechnologies Group, Facilities Management, Administrative Management, the Information Policy Office, and Management Analysis. Elaine Hansen serves as the commissioner of the department.

Audit Scope and Conclusions

Our audit scope was limited to those activities material to the State of Minnesota's Comprehensive Annual Financial Report for the year ended June 30, 1995. We also reviewed selected statewide computer facility general controls, including logical security, disaster recovery, and critical file backup.

We concluded that the Intertechnologies Group is generally controlling access to data and computer resources on the state's two central computers. However, Intertech needs to ensure that agency security officers and liaisons have sufficient technical training to make informed security decisions. We also concluded that, although Intertech provides data processing services, including files backup, storage, and disaster recovery planning, critical state computer applications and data files have not been identified and included in Intertech's disaster recovery testing.

Finally, it is unclear whether Central Motor Pool has complied with Minn. Stat. Section 16B.54, Subd. 8(b), which limits the amount of funds it is allowed to retain. The department needs to seek clarification of the statute to ensure that it complies with the law relating to excess funds.

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

Table of Contents

Audit Participation

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

John Asmussen, CPA	Deputy Legislative Auditor
Jeanine Leifeld, CPA	Audit Manager
Susan Rumpca, CPA	Auditor-in-Charge
Chris Buse, CPA, CISA	Director of Information Systems Audits
Janet Knox, CPA	Auditor
Gail Thurmer, CISA	Auditor
Mark Mathison	Auditor
Margie Caneff	Auditor
Beaujon Guerin	Auditor

Exit Conference

We discussed the findings and recommendations in this report with the following staff of the Department of Administration on January 19, 1996:

Elaine Hansen	Commissioner
Dennis Spalla	Assistant Commissioner, Facilities Management Bureau
Sheila Reger	Director, Human Resources
Fred Grimm	Director, Management Analysis Division
Kent Allin	Assistant Commissioner, Operations Management Bureau
Bernard Conlin	Assistant Commissioner, Intertechnologies Group
Larry Freund	Acting Director, Bureau of Administrative Services
Beverly Schuft	Assistant Commissioner, Information Policy Office
Veronica Legan	Principal Accounting Supervisor
Marcia Hansen	Executive Assistant

Chapter 1. Introduction

The Department of Administration is responsible for providing business management and administrative services to state and local government agencies. Its programmatic areas include Operations Management, the Intertechnologies Group, Facilities Management, Administrative Management, the Information Policy Office, and Management Analysis. The department's primary funding source is self-supporting, fee-based operations. Other funding sources include General Fund appropriations, gifts, and federal grants. During fiscal year 1995, the department expended about $244 million, including about $80.5 million of construction expenditures.

Our scope was limited only to those aspects of the Department of Administration financial activities which are material to the financial activities of the State of Minnesota for the year ended June 30, 1995. The activities which are material to the financial activities of the state are shown in Table 1-1.

Table 1-1
Audited Financial Activities
Year Ended June 30, 1995

Revenue Programs	
Intertechnologies Fund fee revenue	$56,812,536
Plant Management Fund lease revenue	24,304,121
Plant Management Fund transfers	8,771,523
Risk Management Fund insurance revenue	3,396,543
Central Motor Pool Fund rental revenue	6,123,229
Central Stores Fund sales revenue	7,112,240
Printing Services Fund fee revenue	5,616,191
Expense/Expenditure Programs	
Intertechnologies Fund fixed asset purchases	12,103,174
Central Motor Pool Fund fixed asset purchases	6,256,123
Intertechnologies Fund data processing services	17,240,117
Building Construction Division expenditures (selected)	70,859,013

Source: State of Minnesota Comprehensive Annual Financial Report for the year ended June 30, 1995, except for building construction expenditures, which were based on auditor analysis of certain project accounts for the period from July 1, 1994 through June 30, 1995.

The Department of Administration sets rates based on anticipated usage and estimated expenses for some of the programs we audited. The Department of Finance has statutory responsibility to approve the fee rates these programs charge. We did not look at the rate setting process for any of the programs.

The Department of Administration is also responsible, pursuant to Minn. Stat. Section 16B.14, for integrating and operating the state's computer facility. As part of our audit, we reviewed selected computer facility general controls, including logical security, disaster recovery and critical file backup.

Department of Administration

The primary objective of the Statewide Audit is to render an opinion on the State of Minnesota's financial statements included in its Comprehensive Annual Financial Report for fiscal year 1995. This includes whether the financial statements of the state present fairly its financial position, results of operations, and changes in cash flows in conformity with generally accepted accounting principles. As part of our work, we are required to gain an understanding of the internal control structure and ascertain whether the state complied with laws and regulations that may have a material effect on its financial statements.

To address this objective, we interviewed key department employees, reviewed applicable policies and procedures, tested representative samples of financial transactions, and performed analytical procedures, as appropriate.

Our work in the Department of Administration was completed as part of our audit to express an opinion on the state's fiscal year 1995 financial statements. The Comprehensive Annual Financial Report for the year ended June 30, 1995 includes our report issued thereon dated December 1, 1995. The Minnesota Financial and Compliance Report on Federally Assisted Programs for the year ended June 30, 1995 will include our reports on internal control structure and compliance with laws and regulations. We anticipate issuing this report in June 1996.

In addition to preparing standard reports, we have also developed audit findings and recommendations. In Chapters 2-4, we discuss our findings for the Department of Administration.

Chapter 2. Controlling Access to Data and Computer Resources

Chapter Conclusions

The Department of Administration's Intertechnologies Group (Intertech) and state agencies jointly control access to data and computer resources on the state's two central mainframes. In general, we believe that Intertech's Security Services team is restricting the use of powerful ACF2 privileges. Intertech also is limiting the use of powerful privileges that can bypass or compromise security. Finally, it is ensuring that authorized agency employees approve all ACF2 rule and logon ID changes.

However, administering security is very complex and is not exclusively Intertech's responsibility. Rather, it must be a joint effort between Intertech and the agencies who use the state's two central mainframes. Intertech's Security Services Team currently places a great deal of reliance on the competence of decentralized agency security officers and security liaisons. In some instances, we do not feel that these groups have a sufficient understanding of ACF2, the state's security software package. Intertech needs to ensure that the groups on which it relies have sufficient technical training to make informed security decisions. Intertech also needs to give these groups the necessary access to manage their own security.

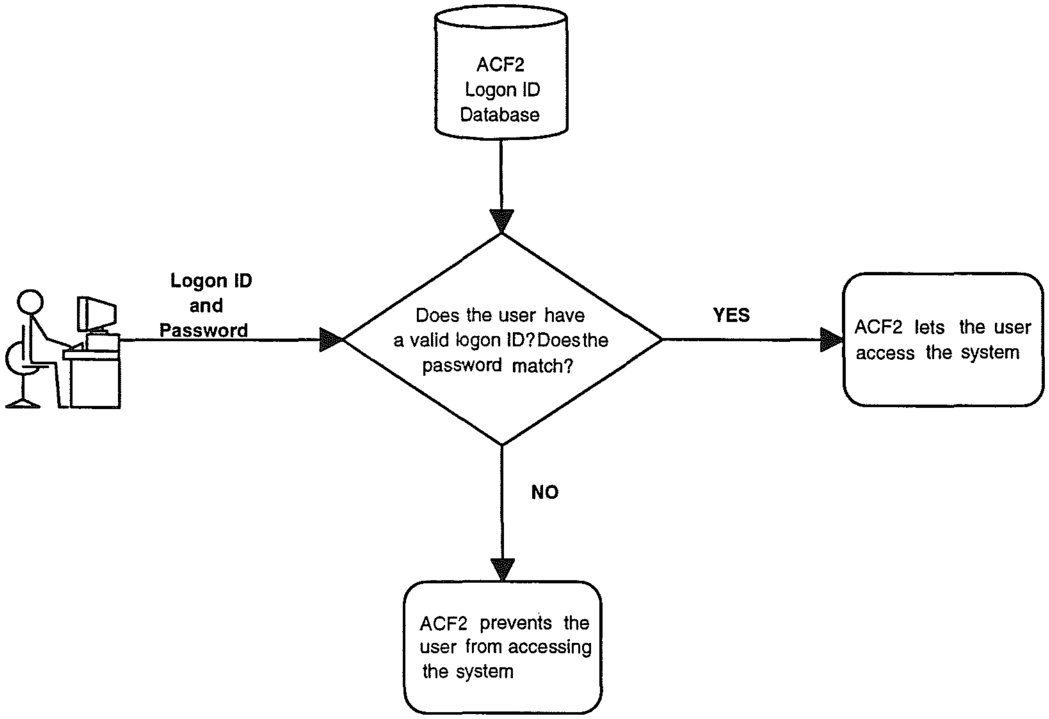
Intertech uses a software package called ACF2 to control access to the state's two central mainframe computers. ACF2 protects against unauthorized destruction, disclosure, modification, or use of data and computer resources. The software acts as an extension to the computer's operating system and protects all data by default. ACF2 will not permit a user to access data or use a computer resource, such as an on-line screen, unless the data owner explicitly authorizes that access.

The Functions of ACF2

ACF2 controls access at two primary levels. The software secures initial access to the system and it secures access to data and resources within the system.

ACF2 uses unique logon IDs and passwords to control access to the system. All users must enter their logon ID and password to access one of the state's central mainframes. ACF2 compares this user information to data stored in its logon ID database. The software denies access to users with unknown logon IDs or incorrect passwords. It also denies access to users with canceled or suspended logon IDs. Figure 2-1 illustrates in a simplified form how ACF2 uses logon IDs and passwords to control initial access to the system.

Figure 2-1
ACF2 Controls Initial Access to the State's Central Mainframes



Source: Auditor prepared.

ACF2 uses rules to control access to data and computer resources. ACF2 makes either an allow or deny decision each time a user tries to access data or use a computer resource, such as an on-line screen. In general, users cannot access any data or use computer resources unless permitted by a rule. However, some users with powerful "privileges", such as the security privilege, can bypass ACF2's rule validation process. However, all actions taken by these users are recorded and subject to review.

Security officers write rules that ACF2 uses to make its allow or deny decisions on behalf of data owners. They also may grant privileges to some users who need them to fulfill their job responsibilities. ACF2 stores all rules in two internal databases - one containing data access rules and another containing computer resource access rules. The software stores each user's privilege information in their logon ID record. Figure 2-2 illustrates in a simplified form how ACF2 uses rules and privileges to control access to data and computer resources.

Audit Scope and Objectives

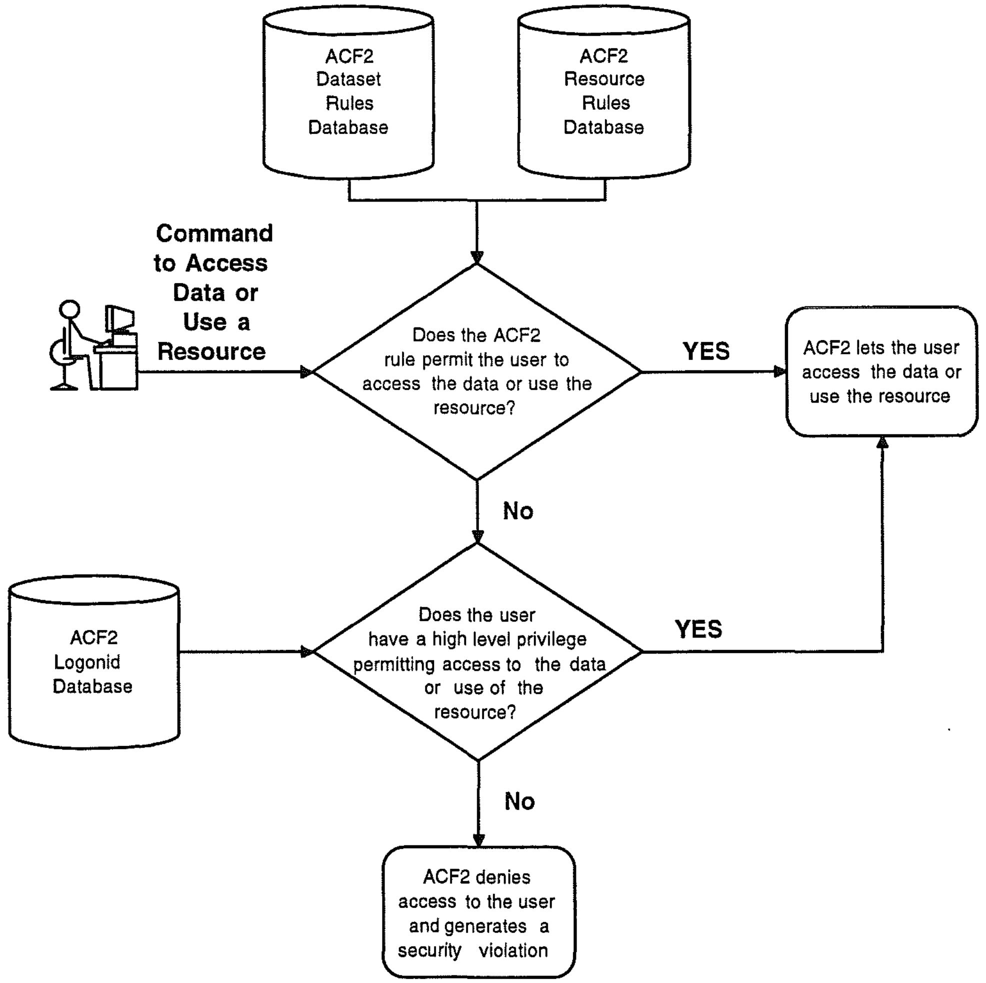
In this chapter, we examine procedures for giving users powerful ACF2 privileges, such as security. We also examine procedures for writing ACF2 data and computer resource rules. The following are our specific audit objectives:

- Is Intertech giving powerful ACF2 privileges to only those employees who need them to fulfill their job responsibilities?

- Is Intertech limiting the scope of privileged users, when appropriate?
- Does Intertech have procedures to ensure that appropriate individuals are approving all ACF2 rule changes?

To answer these questions, we interviewed members of Intertech's Security Services Team and reviewed ACF2 security records. We also interviewed several Intertech managers and decentralized agency security officers located at the Departments of Revenue, Human Services, and Transportation. Finally, we interviewed three agency security liaisons for the Department of Public Safety.

Figure 2-2
ACF2 Controls Each Attempt to Access Data or Use a Computer Resource


ACF2 Dataset Rules Database
ACF2 Resource Rules Database
Command to Access Data or Use a Resource
Does the ACF2 rule permit the user to access the data or use the resource?
YES
ACF2 lets the user access the data or use the resource
No
ACF2 Logonid Database
Does the user have a high level privilege permitting access to the data or use of the resource?
YES
No
ACF2 denies access to the user and generates a security violation

Source: Auditor prepared.

ACF2 Privileges and Scope Lists

Most users need one or more data access privileges to fulfill their job responsibilities. For example, security officers frequently give the "CICS" privilege to people who enter on-line transactions. Without this privilege, these users cannot access IBM's Customer Information Control System (CICS).

Some ACF2 privileges, such as "security", are very powerful and must be tightly controlled. The security privilege indicates that a user is an ACF2 security officer. Unscoped security officers can access all data sets, protected programs, and computer resources. Security officers also can create, change, and delete ACF2 rules and logon ID records. Table 2-1 describes some powerful ACF2 privileges which we reviewed during our audit.

Table 2-1
Powerful ACF2 Privileges Reviewed During Our Audit

Privilege Name	Privilege Description
SECURITY	Indicates that this user is an ACF2 security officer. Security officers have unrestricted access to data, protected programs, and computer resources. Security officers can create, maintain, and delete ACF2 access rules and logon ID records.
ACCOUNT	Indicates that this user can insert, delete, and change logon ID records.
NON-CNCL	Indicates that this user cannot be canceled for ACF2 security violations.
READALL	Indicates that this user can read all data.
MAINT	Indicates that this user can access all data without ACF2 rule validation. However, the user must use a specific program which resides in a predefined library. Also, this program must identify the specific data to access.

Note: This table only lists the five powerful ACF2 privileges that we reviewed during our audit. We selected these privileges because they give users the ability to bypass or change ACF2's rule validation process. ACF2 has many other privileges that we did not review.

ACF2 has a feature, called a "scope list", which security officers can use to limit the authority of users with the most powerful privileges such as "security," "account," and "leader." Scoping is very important in an environment, such as Intertech's, which relies on both centralized and decentralized security administration. Intertech's security officers do not have an ACF2 scope list. This means that they have unfettered access to all data and computer resources. They also can create, modify, or delete any logon ID records. The Departments of Revenue, Transportation, and Human Services have their own "scoped" ACF2 security officers. These scoped security officers perform many of the same duties as Intertech's Security Services Team. However, ACF2 scope lists only let them administer security for their own agencies.

Department of Administration

In general, we feel that Intertech's Security Services Team is restricting the use of powerful ACF2 privileges. We also feel that Intertech is scoping privileged users, when appropriate. However, during our review of ACF2 privileges we found two security concerns that Intertech needs to address. Findings 1 and 2 discuss these concerns.

1. Three Intertech help desk employees have an inappropriate ACF2 privilege.

Intertech gave three help desk employees a powerful privilege which they do not need to fulfill their job responsibilities. Intertech gave its help desk employees the "account" privilege so they can help users with simple logon ID and password problems. However, these employees could perform their duties with a less powerful privilege called "leader". Typical problems encountered by help desk employees include unsuspending logon IDs, changing passwords, and restoring password violation counts. The leader privilege will let a user perform all of these functions.

"Account" is a very powerful privilege because it gives a user the ability to create new logon IDs. When unscoped, a user with the "account" privilege can create logon IDs that can compromise security. None of the three help desk employees with the "account" privilege have an ACF2 scope list.

Recommendation

- *Intertech should assign its help desk employees the minimum ACF2 privilege necessary to fulfill their job responsibilities.*

2. One ACF2 scope list for decentralized security officers at the Department of Human Services is too broad.

Five of the six decentralized security officers at the Department of Human Services have the same ACF2 scope list, named "DHS". However, all of the department's security officers have unique responsibilities. Therefore, we feel that it would be more appropriate to design custom scope lists for each security officer.

Intertech began, but did not finish, the process of designing unique scope lists for the Department of Human Services' decentralized security officers. In fiscal year 1995, Intertech developed a unique ACF2 scope list for one security officer. Previously, all six security officers shared the same scope list. However, Intertech did not change the original DHS scope list after designing this new list. As a result, the five security officers governed by the original DHS scope list still have more authority than they need. For example, the DHS scope list gives these five security officers the authority to write ACF2 computer resource rules. None of these decentralized security officers need this authority to fulfill their job responsibilities.

Scope lists are an important control because they limit the authority of users with powerful ACF2 privileges. Therefore, it is important to design scope lists which correspond with security officer's specific job responsibilities.

Recommendation

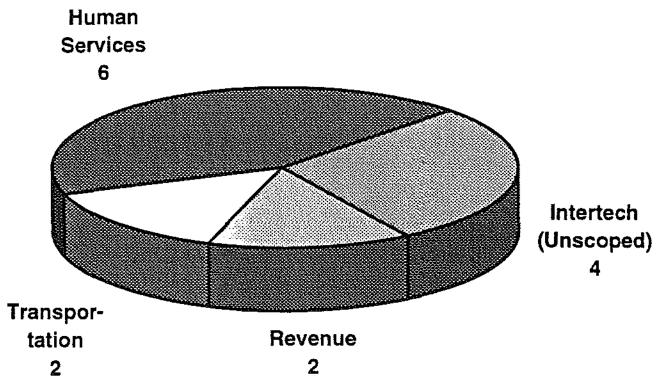
- *Intertech should restrict the scope of distributed security officers to the minimum clearance necessary to fulfill their job responsibilities.*

Writing ACF2 Access Rules

Security officers are responsible for writing ACF2 access rules. In total, there are 14 security officers who control access to the state's two central mainframes. Intertech has the only unscoped security officers. This gives Intertech the ability to control all aspects of ACF2 centrally. Intertech also maintains a list of agency security liaisons. These security liaisons communicate ACF2 security decisions to Intertech. Currently, there are 110 security liaisons from 44 different state agencies.

Intertech delegates some of its authority to decentralized agency security officers. Figure 2-3 illustrates the breakdown of the state's ACF2 security officers by agency.

Figure 2-3
Breakdown of ACF2 Security Officers By Agency
As of September 30, 1995



Source: Data obtained through ACF2 inquiries.

Some decentralized security officers write all of their own rules. However, most rule writing is still a joint effort between Intertech and the other user agencies. Security liaisons and decentralized security officers communicate access decisions to Intertech. Intertech then writes rules to implement those security decisions.

We interviewed Intertech's Security Services Team and the decentralized security officers to discuss ACF2 rule writing procedures. These security officers verified that appropriate individuals approve changes to ACF2 rules. They also have acceptable procedures for documenting those approvals. However, several factors may limit the effectiveness of this system of mutual reliance. First, there are no formal training requirements for agency security liaisons or decentralized security officers. Also, Intertech does not give agency security liaisons the necessary clearance to review their own rules. Findings 3 and 4 discuss these concerns in more detail. Finding 5 discusses concerns we have with groups of Intertech employees who have unrestricted access to data owned by other agencies.

3. The state does not have training guidelines for agency security liaisons or decentralized security officers.

Some agency security liaisons and decentralized security officers we interviewed do not have a sufficient understanding of ACF2. Intertech's Security Services Team is not in a position to understand the technical intricacies of all systems residing on the state's two central mainframes. It also cannot judge what clearance agency employees need to fulfill their job responsibilities. Therefore, Intertech must rely on decisions made by decentralized agency security officers and security liaisons. This reliance may result in problems, however, when decentralized agency security officers and security liaisons have not been properly trained.

We found several cases where decentralized security officers at the Department of Human Services did not understand the ramifications of their decisions. For example, the department told Intertech to give the ACF2 security privilege to three computer programmers. It made this decision to provide a secondary level of back up for its three regular ACF2 security officers. Normally, the department's three regular security officers serve as back ups for each other. The department's lead security officer did not realize that this privilege would let the programmers bypass ACF2 access rules.

We have similar concerns with the security liaisons we interviewed from the Department of Public Safety. These employees communicate access requests to Intertech and review daily ACF2 security reports. However, none of these security liaisons has ever seen an ACF2 rule or taken any training. As a result, the liaison responsible for reviewing daily ACF2 security reports does not understand some of the reports. Also, there are weaknesses in the Motor Vehicle System's ACF2 access rules. One rule gives every Public Safety employee clearance to read all Motor Vehicle System data. This gives a large group of employees the ability to view or make unauthorized copies of confidential data. Another rule gives employees from the Office of the Legislative Auditor clearance to update or delete Motor Vehicle System data. Auditors only need clearance to read data. Finally, the department did not specify expiration dates for some temporary access rules. Therefore, some users who only needed temporary clearance now have permanent access to the Motor Vehicle System.

Decisions made by decentralized security officers and security liaisons have a major impact on the state's two central mainframe computers. Therefore, we think that it is important to develop formal training policies for these groups.

Recommendation

- *The Department of Administration should develop formal training policies for decentralized agency security officers and security liaisons.*

4. Some agency security liaisons do not have a privilege needed to manage their ACF2 rules.

Intertech does not give agency security liaisons clearance to view their ACF2 access rules. Agency security liaisons rely on members of Intertech's Security Services Team to write their ACF2 access rules. However, these security liaisons cannot view their own rules to verify the accuracy and completeness of Intertech's work. Under this system, rule writing and communication errors can occur and remain undetected.

The three security liaisons we interviewed from the Department of Public Safety had never seen their ACF2 security rules. Therefore, they were unaware of the weaknesses described in finding 3. Intertech could improve controls over ACF2 rules by giving security liaisons the privilege to allow users to read, but not change, ACF2 access rules.

Recommendation

- *Intertech should help agency security liaisons manage their ACF2 rules by giving them the privilege to review their rules.*

5. Intertech assigns some of its employees unrestricted access to data that belongs to other agencies.

Some groups of Intertech employees have unrestricted access to other agencies' data. With this access, they can read, change, or even delete some of the most sensitive data in the state. We recognize that some employees need this authority to fulfill their job responsibilities and help agencies in emergency situations. However, other employees in these groups may not need this broad level of authority. Intertech needs to review the authority granted to employees in these powerful groups on an ongoing basis. It also should explore alternative methods to control these powerful users.

Intertech designed new security groups four years ago. Since that time, Intertech has undergone several reorganizations. However, it did not update its security groups to reflect these organizational changes. Intertech managers told us that they are now initiating a comprehensive project to review all security groups.

Giving individual employees continuous and unrestricted access to other agencies' data has significant risks. Therefore, we think that Intertech should explore other methods that only give employees access when needed. One possibility may be to start using a "firecall" logon ID. A firecall logon ID is a powerful logon ID that employees can use in emergency situations. Supervisors or security officers typically retain custody of the password and change it frequently. Intertech has not used its firecall logon ID for several years. Another possibility may be to use an ACF2 concept called "program pathing". Program pathing includes giving employees access to specific tools that they need to perform their job responsibilities. It also includes placing restrictions on the tool's environment.

Recommendations

- *Intertech should review its security groups on an ongoing basis.*
- *Intertech should explore other methods to control its powerful users.*

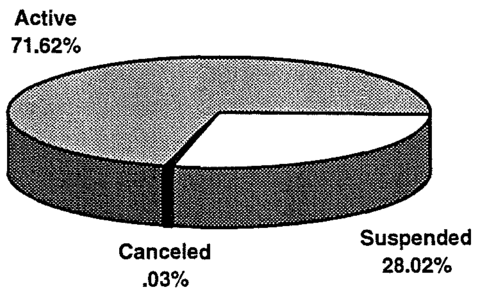
Other Issues

Several other issues came to our attention during our work done on ACF2 rule writing and privileges. First, Intertech needs to develop procedures for maintaining ACF2's logon ID and access rule databases. Findings 6 and 7 discuss these issues. Also, Intertech does not require all of its employees to change their passwords. Finding 8 discusses this issue.

6. The ACF2 logon ID database contains a large number of canceled and suspended logon ID records.

Intertech does not have procedures for deleting canceled and suspended logon IDs. As a result, the ACF2 logon ID database contains an unusually large percentage of logon IDs that are in canceled and suspended status. The ACF2 logon ID database had 25,877 records at the conclusion of our audit. As Figure 2-4 illustrates, approximately 28 percent of these logon ID records are either canceled or are in suspense.

Figure 2-4
Percentage of Logon IDs in Canceled or Suspended Status
As of December 5, 1995



Source: Data obtained through ACF2 logon ID database inquiries.

Intertech needs to develop procedures to cancel logon IDs in suspense status. It also needs to develop procedures for deleting logon IDs in canceled status. Currently, Intertech simply suspends logon IDs that have not been used for over 90 days.

It is possible to use suspended logon IDs to compromise security. For example, a user with the "leader" privilege could unsuspend one of these logon IDs and assign it a new password. This would let the user assume the identity and access rights assigned to the logon ID's original owner.

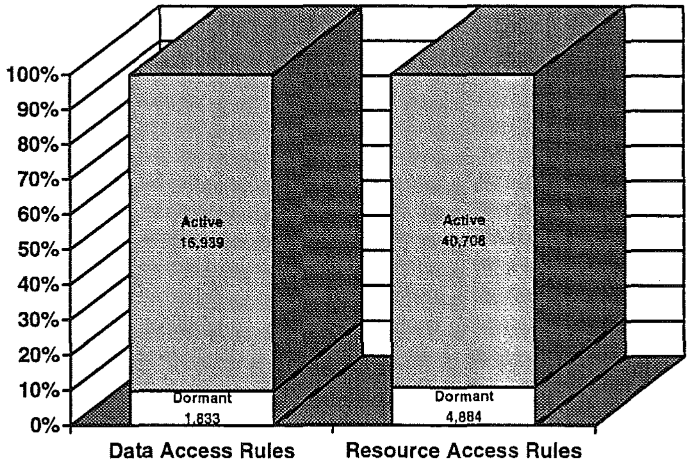
Recommendation

- *Intertech should develop maintenance procedures for canceled and suspended logon IDs.*

7. The two ACF2 rule databases contain a large number of outdated rules.

Intertech does not have procedures for deleting outdated ACF2 rules. As a result, the two ACF2 rule databases contain a large number of "dormant" rules. Dormant rules are rules that cannot grant or restrict access to any user. The ACF2 data access rule database had 18,915 rules at the close of our audit and the ACF2 computer resource rule database had 45,696 rules. However, dormant rules account for approximately 9.69 and 10.60 percent of the rules in each of these databases, respectively. Figure 2-5 illustrates the percentage of dormant rules in each of the two ACF2 rule databases.

Figure 2-5
Analysis of Dormant ACF2 Data and Computer Resource Rules
As of December 5, 1995



Source: Data obtained from ACF2 rule database inquiries.

Dormant rules can lead to future ACF2 security problems. New logon IDs which happen to meet the criteria specified in a dormant rule can access the data or resource that the rule was originally intended to protect. Therefore, it is important to periodically remove all dormant rules from the ACF2 rule databases. Intertech has a tool, called ETFA, that can identify and remove dormant rules. However, the Security Services Team has not used ETFA for this purpose.

Recommendation

- *Intertech should periodically remove dormant rules from the two ACF2 access rule databases.*

8. Intertech does not require some of its employees to change their passwords.

We found 26 Intertech employees who do not have to change their passwords. ACF2 has a feature, called "maxdays", which forces users to periodically change their passwords. The 26 employees we identified do not have a maxdays parameter in their logon ID records. Therefore, ACF2 does not prompt them to change their password after a certain number of days. One employee with the ACF2 "security", "account", and "non-cncl" privileges has used the same password since 1987.

ACF2 uses unique logon IDs and passwords to control access to the state's two central mainframes. Periodically changing passwords is a key control to prevent and detect unauthorized system users.

Recommendation

- *Intertech should require all employees to periodically change their passwords.*

This page intentionally left blank.

Chapter 3. Computer Backup and Recovery

Chapter Conclusions

The Intertechnologies Group provides data processing services, including file backup, storage, and disaster recovery planning, for those state agencies processing data on the centralized mainframe computers. However, each state agency, as the data owner, is responsible for maintaining the security and recoverability of its own information assets. Although required by Minn. Stat. Section 16B.41, subd. 2(f)(2), the Information Policy Office has not adopted specific standards and guidelines for disaster recovery. The state has not identified and prioritized its critical applications and data files for recovery in the event of a disaster and assured that Intertech includes all critical applications and data sets in its periodic disaster recovery tests. The Department of Administration's disaster recovery plan does not ensure that the state's most critical data files could be recovered in the event of a disaster.

The Intertechnologies Group (Intertech) provides centralized data processing for state agencies such as the Departments of Finance, Revenue, Human Services, Transportation, Public Safety and others. Information systems are critical to the mission of these state agencies. Agency applications process accounting and payroll transactions, benefit payments, tax collections, motor vehicle registrations and numerous other state operations.

Intertech has taken significant steps to provide back-up and recovery services for state agencies processing data on the centralized mainframe computers These services include disaster recovery planning, file backup, and off-site storage. Administration has developed a disaster recovery plan for its mainframe computers and tested the plan four times during fiscal year 1995 at an alternate site. Intertech operates an off-site data storage facility and performs routine back-ups of data files on a weekly basis. It also provides agencies with specialized software to assist in tracking and restoring back-up files.

Despite the steps taken by Administration, we do not believe that the state's data is adequately protected in the event of a disaster.

9. PRIOR FINDING NOT RESOLVED: Critical state computer applications and data files have not been identified and included in Intertech's disaster recovery testing.

The state has not identified and prioritized the critical applications and related data files necessary for the state to operate and recover after a disaster. There has not been a forum for performing a "statewide" assessment of risk to identify which applications and data files should be recovered first in the event of a disaster.

Department of Administration

It may be possible for Intertech to restore data files without the help of the data owners; however, systems may not be recovered in a timely manner. Some state agencies have been unwilling to participate in Intertech's disaster recovery plan testing. Due to this lack of collaboration, the tests have not included all applications and data files.

We believe that the Department of Administration has the authority and responsibility to initiate a statewide forum to identify critical state applications and data files. Minn. Stat. Section 16B.41, Subd. 2(f)(2) and (i) states, "The office [Information Policy Office], in consultation with the intergovernmental information systems advisory council and the legislative reference library, shall adopt specific standards and guidelines to be met by each state agency within a time period fixed by the office in regard to the following: . . . establishment of data retention schedules, disaster recovery plans and systems, security systems, and procedural safeguards concerning privacy of data."

As the data owner, each agency is responsible for deciding when and how data files are backed up and stored. Many of the state's data files are not being tracked by Intertech's back-up and recovery software. The software, called SUNRISE, identifies and restores backup files. If agencies do not choose to track their files through SUNRISE, it is unlikely the application and data files could be restored in a timely manner.

Recommendations

- *The Information Policy Office should adopt specific standards and guidelines with regard to disaster recovery plans and monitor state agencies' progress towards meeting those requirements.*
- *Administration should initiate a risk assessment of critical mainframe applications and help agencies prioritize them for recovery.*

Chapter 4. Central Motor Pool

Chapter Conclusions

Central Motor Pool's fixed assets and vehicle rental revenues as reported in the state's financial statements are fairly stated in compliance with generally accepted accounting principles. It is unclear, however, whether Central Motor Pool has complied with Minn. Stat. Section 16B.54, Subd. 8(b), which limits the amount of funds it is allowed to retain.

The Travel Management Division offers three major services to state agencies. First, Central Motor Pool provides daily, weekly and monthly vehicle rentals, including vehicle maintenance and repair. Second, the division provides a fleet of passenger vans for state employees who commute to work in a van pool. Finally, the division offers a corporate credit card program, preferred travel vendors, and monthly bus cards through a payroll deduction program for state employees. Minn. Stat. Section 16B.54 establishes Central Motor Pool and the Motor Pool Fund. We limited our scope to a review of Central Motor Pool fixed asset purchases, disposals, and depreciation, as well as a review of vehicle rental revenue.

Central Motor Pool reported a fixed assets balance of $12,357,433 as of June 30, 1995. The amount presented in the state's financial statements was fairly stated in compliance with generally accepted accounting principles. Vehicles comprise 98 percent of Central Motor Pool's total fixed assets. During our audit of Central Motor Pool's fixed assets, we reviewed the acquisition, disposal and inventory management of vehicles. The Department of Administration holds title to all vehicles acquired by Central Motor Pool. Central Motor Pool disposes of its used vehicles at public auctions.

Central Motor Pool receives most of its revenues through daily, weekly and monthly vehicle rental to state agencies. Central Motor Pool charges customers a daily or monthly rate plus a variable rate. The variable rate is based on mileage. The rates cover gasoline, oil, tires, normal operating maintenance and insurance costs. Central Motor Pool reported vehicle rental fees of $6,123,229 on the state's financial statements.

Our audit of Central Motor Pool identified one instance of potential noncompliance.

10. The Motor Pool Fund had cash on hand at June 30, 1995 potentially in excess of the statutory limit.

Central Motor Pool may not have complied with Minn. Stat. Section 16B.54, Subd. 8(b), which limits the "unobligated amounts" the Motor Pool Fund can retain. This statute specifies that "unobligated amounts in the state treasury in excess of $438,000" must be transferred at fiscal year end to the General Fund. Central Motor Pool has not made any transfers to the General Fund under this provision. The fund had a cash balance at June 30, 1995 of $506,636. Considering the fund's outstanding encumbrances at June 30 of $178,055, Motor Pool's unencumbered balance as of year end was $328,581. In addition, the fund had current and long-term liabilities exceeding $12.5 million at June 30, including master lease payments to the Department of Finance in excess of $400,000. The statutes do not define the term, "unobligated amounts." It could be construed as the cash balance or the unencumbered balance or some other amount. Therefore, it is unclear whether the Central Motor Pool Fund complied with Minn. Stat. Section 16B.54, subd. 8(b).

Recommendation

- *The Department of Administration needs to seek clarification of Minn. Stat. Section 16B.54, Subd. 8(b) to ensure that it complies with the law relating to excess funds. If deemed necessary, the Central Motor Pool Fund should transfer its excess cash to the General Fund.*

STATE OF MINNESOTA

Department of Administration

Our mission:
To improve the quality
and productivity
of Minnesota
government.

February 2, 1996

Mr. Jim Nobles
Legislative Auditor
First Floor, Centennial Office Building
658 Cedar Street
St. Paul, MN 55155

Dear Jim:

In reviewing our FY95 audit report, we would like to respond to recommendations in Chapters 2, 3, and 4, involving InterTech, IPO and Travel Management.

INTERTECHNOLOGIES GROUP

1. **Help Desk employees' ACF2 privilege.**

RESOLVED. During the audit, the more powerful privilege "account" was changed to the less powerful privilege "leader."

2. **Department of Human Services' ACF2 scope list.**

RESOLVED. During the audit, DHS reviewed the scoping of their security administrators and had InterTech revise the scoping. DHS scope limiting is based on their security administrator backup needs and providing security administration 7 days a week, 24 hours a day. DHS will periodically review their scope lists.

3. **Training guidelines for agency security liaisons or decentralized security officers.**

RESOLVED. Current training practices involve initial one-on-one training with new security administrators. InterTech also recommends that the administrators take the ACF2 Administrators Training offered by EKC, Inc. InterTech's security team also informs agency security administrators of new ACF2 releases, consults with agency security administrators, and notifies security administrators of conferences and training related to security. However, agency management must recognize its accountability for the security of its data under the provisions of IPO Administrative Policy & Procedure No. 309 and Minnesota Statutes Chapter 16B.40, subd. 8, and Chapter 13.05, subd. 5, and provide sufficient support to the security operation within their respective agencies to ensure that it is adequately staffed and that staff is properly trained. InterTech will formalize current ACF2 security training practices and provide them to agency management, agency security officers and agency security liaisons.

4. Agency security liaison privileges.

POLICY. The recommendation of this finding is to give the "audit" privilege to some of the agency security liaisons. "Audit" authority gives people more security browse authority than is necessary for them to effectively do their jobs.

InterTech will review alternate methods of providing security browse privileges to agency security liaisons. The alternate methods will then be available to agencies requiring security browse privileges.

5. Employee access to data of other agencies.

POLICY. The groupings of InterTech support personnel are designed to provide support personnel backup, application support coverage 7 days a week, 24 hours a day, and disaster recovery support. InterTech does not manage the access of support personnel. With the approval of agency responsible authorities, the support groups have less restrictive access to data and resources, but these accesses are logged and reviewed every day by InterTech and other state security administrators.

These groupings reflect job and functional responsibility; they do not reflect organizational boundaries and are not affected by reorganizations.

Using "firecall" IDs as recommended may be impractical, as in many cases, InterTech would lose individual accountability.

Program pathing would create problems when InterTech changes program tools in their environment.

InterTech will continue to periodically review and adjust support personnel access privileges. This review will be conducted with client agencies where necessary.

6. ACF2 logonid database contains a large number of canceled and suspended records.

POLICY. InterTech will provide clients with listings of logonids that have been suspended or canceled for more than one year. These listings must be reviewed by the agencies owning the logonid and the agency must determine the disposition of the logonid. InterTech cannot automate the disposition of canceled and suspended logonids.

7. **ACF2 outdated rules.**

POLICY. InterTech cannot remove dormant rules until the data and resources controlled by these rules are removed. Where agency data and resources are involved, InterTech must consult with the agency. InterTech will provide clients with listings of dormant data and resource access rules. These listings must be reviewed by the agencies owning the data and resources, and the agency must determine the disposition of these resources.

8. **InterTech does not require some of its employees to change their passwords.**

RESOLVED. A review of logonids will be performed and password expiration adjustments will be made where appropriate.

9. **PRIOR FINDINGS NOT RESOLVED: Critical state computer applications and data files have not been identified and included in InterTech's disaster recovery testing.**

RESOLVED. InterTech has been working with state agencies to prioritize critical applications for the past several years. InterTech has received confirmation from the Department of Human Services and anticipates confirmation from the Department of Revenue shortly. Based on input from state agencies, InterTech will continue to prepare a pro forma list of critical applications. This list will be circulated to all state agencies for their confirmation.

INFORMATION POLICY OFFICE

Recommendation: The Information Policy Office should adopt specific standards and guidelines with regard to disaster recovery plans and monitor state agencies' progress toward meeting those requirements.

POLICY. Administrative Policy No. 309--Information Asset Security-- was issued under Commissioner Dana B. Badgerow, effective May 1992.

The protection of information assets is considered a management function. "The commissioner or head of each department or agency is ultimately responsible for the information assets held by that agency and responsible for assuring an adequate level of security. The commissioner of each agency must designate one person who is accountable for security in that agency. If a disastrous loss of information assets occurs, a timely recovery of critical resources must be possible. Each agency is responsible for ensuring that a sufficient disaster recovery capability exists to meet this requirement." IPO does not audit agency disaster recovery plans.

In the rapidly changing technology environment, and with a broad array of systems and platforms, rigid use of specific standards is not usually effective. IPO supports the use of "Security Best Practices" for guiding agencies in the development of their plans. Agencies must identify and assess their risks, develop plans to mitigate those risks, provide adequate training, and monitor and enforce those plans.

IPO is not in a position to identify and prioritize critical state applications and related data files necessary for the state to operate and recover after a disaster. "Critical applications" will depend on the nature, location and magnitude of the disaster and someone other than IPO, most likely the Governor's Office, would be making those decisions.

CENTRAL MOTOR POOL

10. Cash on hand at June 30, 1995.

POLICY. Minnesota Statute 16B.54, subd. 8(b) requires that "unobligated amounts in the state treasury in excess of $438,000" must be transferred at fiscal year end to the General Fund. The audit correctly reflects the fund's FY95 year-end cash of $506,636 with outstanding encumbrances at $178,055 and current and long-term liabilities in excess of $12.5 million. It is our position that the current and long-term liabilities, resulting from the execution of various master lease finance agreements for vehicle and equipment purchases, represent a fund obligation. As such, the Central Motor Pool is in compliance with statutory requirements.

We would like to take this opportunity to commend your staff for their professionalism during the audit and the exit conference and for their willingness to discuss our various concerns following that meeting.

Sincerely,

Elaine S. Hansen
Commissioner

esh/mh
c: John Asmussen
Jeanine Leifeld