OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial-Related Audit

Department of Administration Intertechnologies Group

System-wide Access to Mainframe Data

OCTOBER 19, 2000 **00-49**

Financial Audit Division

The Office of the Legislative Auditor (OLA) is a professional, nonpartisan office in the legislative branch of Minnesota State government. Its principal responsibility is to audit and evaluate the agencies and programs of state government (the State Auditor audits local governments).

OLA's Financial Audit Division annually audits the state's financial statements and, on a rotating schedule, audits agencies in the executive and judicial branches of state government, three metropolitan agencies, and several "semi-state" organizations. The division also investigates allegations that state resources have been used inappropriately.

The division has a staff of approximately fifty auditors, most of whom are CPAs. The division conducts audits in accordance with standards established by the American Institute of Certified Public Accountants and the Comptroller General of the United States.

Consistent with OLA's mission, the Financial Audit Division works to:

- Promote Accountability,
- Strengthen Legislative Oversight, and
- Support Good Financial Management.

Through its Program Evaluation Division, OLA conducts several evaluations each year and one best practices review.

OLA is under the direction of the Legislative Auditor, who is appointed for a six-year term by the Legislative Audit Commission (LAC). The LAC is a bipartisan commission of Representatives and Senators. It annually selects topics for the Program Evaluation Division, but is generally not involved in scheduling financial audits.

All findings, conclusions, and recommendations in reports issued by the Office of the Legislative Auditor are solely the responsibility of the office and may not reflect the views of the LAC, its individual members, or other members of the Minnesota Legislature.

This document can be made available in alternative formats, such as large print, Braille, or audio tape, by calling 651-296-1727 (voice), or the Minnesota Relay Service at 651-297-5353 or 1-800-627-3529.

All OLA reports are available at our Web Site: http://www.auditor.leg.state.mn.us

If you have comments about our work, or you want to suggest an audit, investigation, evaluation, or best practices review, please contact us at 651-296-4708 or by e-mail at auditor@state.mn.us

OLA

OFFICE OF THE LEGISLATIVE AUDITOR
State of Minnesota • James Nobles, Legislative Auditor

Representative Dan McElroy, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. David Fisher, Commissioner
Department of Administration

We have conducted a financial-related audit of selected activities at the Minnesota Department of Administration's Intertechnologies Group. Our audit scope included a review of system-wide access to data stored on the state's mainframe computers as of June 2000.

We conducted our audit in accordance with *Government Auditing Standards*, as issued by the Comptroller General of the United States. 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 Department of Administration complied with the provisions of laws, regulations, contracts, and grants that are significant to the audit. The department's management is responsible for establishing and maintaining the internal control structure and for compliance with applicable laws, regulations, contracts, and grants.

This report is intended for the information of the Legislative Audit Commission and the management of the Department of Administration. This restriction is not intended to limit the distribution of this report, which was released as a public document on October 19, 2000.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: June 22, 2000

Report Signed On: October 16, 2000

Room 140, 658 Cedar Street, St. Paul, Minnesota 55155-1603 • Tel: 651/296-4708 • Fax: 651/296-4712
E-mail: auditor@state.mn.us • TDD Relay: 651/297-5353 • Website: www.auditor.leg.state.mn.us

Department of Administration
Intertechnologies Group
System-wide Access to Mainframe Data

Table of Contents

Audit Participation

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

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Christopher Buse, CPA, CISA	Audit Manager
Mark Mathison, CPA, CISA	Auditor-In-Charge
Rhonda Regnier, CPA	Auditor

Exit Conference

We discussed the findings and recommendations of the audit with the following representatives of the Department of Administration on September 29, 2000:

David Fisher	Commissioner
Kirsten Cecil	Deputy Commissioner
Jack Yarbrough	Assistant Commissioner
Greg Dzieweczynski	Interagency Services Director
Ray Kermode	Security Services Manager
Ron Michaels	Financial Manager

Department of Administration
Intertechnologies Group
System-wide Access to Mainframe Data

Report Summary

The Department of Administration's Intertechnologies Group (Intertech) used ACF2 security features to limit most system-wide clearances to its own information system professionals and certain installed software products. However, an excessive number of these either have widespread access to data or could obtain this level of clearance through weaknesses in the security infrastructure.

Key Findings:

- ACF2 rules give many Intertech employees and installed software products widespread access to data. (Finding 1, page 7)
- Intertech did not adequately control some powerful ACF2 privileges. (Finding 2, page 7)
- One ACF2 exit may expose data to unauthorized access. (Finding 3, page 8)
- Documentation of key components of the ACF2 security infrastructure is inadequate. (Finding 4, page 8)

Chapter 1. Introduction

This audit focused on people and installed software products that have widespread clearance to data on the state's central mainframe computers. To perform maintenance activities, some information technology professionals in the Department of Administration's Intertechnologies Group (Intertech) need accounts with broad and powerful security clearances. Certain software packages also need accounts with very powerful clearances. Limiting the number and scope of these extremely powerful accounts is a critical security administration responsibility. Unauthorized use of these types of accounts could lead to a disastrous loss or the widespread destruction of data.

The central mainframe computers at Intertech house some of the state's most important business systems and data. These systems help state agencies deliver critical government services, including:

- administering social service programs such as Medical Assistance, Temporary Assistance to Needy Families, and Food Stamps;
- collecting and recording tax payments;
- operating the state's central accounting and payroll systems; and
- licensing drivers and motor vehicles.

Intertech deploys multiple layers of security to protect these business systems and data. For example, Intertech uses security tools to control network connections to its mainframe computers. Intertech also restricts physical access to its mainframe computing facility. One of the most important security layers is a mainframe access control software package called ACF2. ACF2 protects against the unauthorized destruction, disclosure, or modification of data. ACF2 will not permit a person or an installed software product to access data unless a security officer or the data owner explicitly authorizes that access. ACF2 security rules define these explicit authorizations.

Security officers at Intertech have primary responsibility for administering ACF2. However, Intertech delegates some of its security administration duties to distributed security officers who work for several of the largest state agencies. Together, Intertech and these distributed security officers manage over 60,000 ACF2 security rules. They also oversee approximately 24,000 accounts with clearance to access mainframe data. Security officers created many of these accounts for the state agency employees that need to interact with specific business systems. Software products installed on the mainframe use the remaining accounts.

The size and complexity of Intertech's mainframe computing facility creates many security administration challenges. Many state agency business systems must be available seven days per

week and 24 hours per day. When problems arise, information system professionals at Intertech need clearance to help state agencies resume their business operations. The mainframe computers also house a wide variety of complex and interdependent technologies. This means that some information system professionals need security clearances that overlap many technologies. Security officers need to understand these challenges to develop security solutions that give people the clearance that they need, without compromising the system-wide integrity of critical business data.

During this audit, we analyzed how Intertech uses ACF2 to limit system-wide access to data. We also identified and assessed the appropriateness of those accounts with powerful security clearances. Chapter 2 discusses the scope of our work and conclusions that we reached.

Chapter 2. System-wide Access to Data

Chapter Conclusions

An excessive number of people either have widespread access to data or could obtain this level of clearance through weaknesses in the security infrastructure. We found many security rules that grant large groups of information technology professionals and installed software products unnecessarily broad access to data. Many of the people and software products in these security groups may not need this far-reaching clearance. We also found many accounts with powerful privileges that were not properly controlled. Finally, we identified an excessive number of people with access to powerful programs that could be used to circumvent security. If used improperly, these programs could cause significant damage to data housed on the central mainframe computers.

During the course of our work, we also identified documentation shortcomings for the ACF2 security infrastructure. Of greatest significance, security officers could not provide us with written documentation that explains the purpose of and technical contacts for each security rule. We feel that these documentation shortcomings could make future security infrastructure maintenance more challenging, particularly if key security officers leave state service. Documentation shortcomings could also increase the time needed to recover business operations from a disaster.

Intertech uses ACF2 security software to limit system-wide access to data. As illustrated in Figure 2-1, ACF2 will give people or installed software products access to data if any of the following conditions are true:

- ACF2 recognizes the person or the installed software component as the owner of the data. ACF2 gives data owners complete and unfettered access to the data that they own.
- ACF2 security rules explicitly authorize the access.
- The person or installed software product has a special ACF2 privilege that permits them to bypass the normal rule validation process.
- The person or installed software product uses a special computer program, called an "authorized program," to access the data. In some cases, ACF2 does not interfere with access requests made by authorized programs.

- An ACF2 "exit" permits such access. Organizations that install ACF2 can program their own exits to circumvent the security software's normal decision-making process.

Audit Objective and Methodology

We designed our work to answer the following question:

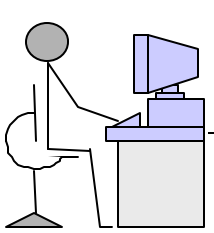
- ***Did Intertech limit system-wide access to data to only those people who need such clearances to fulfill their job responsibilities?***

To answer this question, we interviewed information system professionals and security officers who maintain the ACF2 security software. We also used special tools to analyze the detailed ACF2 security rules that were written to protect critical business data. Finally, we analyzed the ACF2 accounts for all people and installed software products, specifically targeting those with certain powerful ACF2 privileges.

Conclusions

Intertech used ACF2 security features to limit most system-wide clearances to its own information system professionals and certain installed software products. However, as discussed in Finding 1, we found that ACF2 security rules grant large groups of these employees and installed software products unnecessarily broad access to data. We also found many powerful accounts used by these employees and software products that were not properly controlled. Finding 2 discusses our concerns with powerful ACF2 privileges in more detail. In Finding 3, we discuss security risks posed by one ACF2 exit deployed by Intertech. Finally, in Finding 4, we discuss security infrastructure documentation shortcomings that came to our attention.

Figure 2-1
ACF2's Decision-Making Process



Source: Auditor prepared.

1. ACF2 rules give many Intertech employees and installed software products widespread access to data.

Most ACF2 security rules grant large groups of Intertech information system professionals and installed software products complete and unfettered access to data. This data includes agency business data, files and programs essential to the mainframe computer's operating system, and even some ACF2 security data. We recognize that some people and software products need this type of broad access to perform ongoing system maintenance. However, we feel that most could fulfill their typical job duties with more targeted security clearances.

Of particular concern, we found many accounts with clearance to modify "authorized programs." Authorized programs are computer programs that reside in specially defined libraries. Access to these programs and libraries should be tightly controlled because they can be used to circumvent security. We also found an excessive number of accounts with clearance to modify critical operating system components. Normally, only a select few information system professionals with special skills need clearance to modify operating system parameters.

Writing security rules that give large groups of people and software products widespread and continuous access to data exposes the state to significant risks. When questioned, security officers at Intertech told us that they shared our concerns and were actively searching for solutions. These security officers told us that they were currently redefining the membership in existing security groups to make them more concise. They also were exploring ways to only give people temporary access to data, and then revoke that access when no longer needed. However, Intertech security officers had not implemented either of these solutions by the time we completed our work.

Recommendations

- *Intertech should define ACF2 security groups that are appropriate for specific job functions.*

- *Intertech should evaluate the need for powerful group clearances permitted in ACF2 security rules.*

2. Intertech did not adequately control some powerful ACF2 privileges.

Intertech did not implement important mitigating controls for some personal and software product accounts with powerful ACF2 privileges. One ACF2 privilege that we reviewed gives accounts the ability to access data without supplying a password. This privilege provides organizations with a mechanism to schedule and run computer job streams at night. Recognizing the risks posed by accounts with no passwords, the developers of ACF2 designed special compensating controls for security officers to deploy. However, we found many of these privileged accounts on the central mainframe computers at Intertech that did not utilize these important compensating controls. Some of these accounts held other powerful ACF2 privileges

as well, compounding the risks even further. When questioned, Intertech told us that they created many of these powerful accounts before they fully understood how the compensating controls worked.

We also found some people with other powerful privileges that they may not need to fulfill their normal job duties. For example, one person we tested had clearance to access ACF2 to create or modify accounts. When questioned, this person did not realize that he had this clearance. Other people that we reviewed had inappropriate clearances to view ACF2 security rules. Finally, we found one person with inappropriate access to the most powerful ACF2 privilege. This is the privilege that identifies a person as an ACF2 security officer.

Recommendations

- *Intertech should deploy the ACF2 recommended compensating controls over all accounts that do not require passwords.*

- *Intertech should remove powerful ACF2 privileges from those people who do not need those privileges.*

3. One ACF2 exit may expose data to unauthorized access.

Intertech deployed an "exit" that permits access to any data that is not protected by an ACF2 rule. Organizations that install ACF2 can program their own exits to circumvent the security software's standard decision-making process. Normally, ACF2 does not permit a person or an installed software product to access data unless a security officer explicitly authorizes that access in a rule. Fortunately, Intertech has ACF2 rules that protect most critical business data on the central mainframe computers. Furthermore, this exit permits "read-only" access to all remaining unprotected data. However, when questioned, Intertech was unable to justify the need for this exit that bypasses ACF2's normal decision-making process.

Recommendation

- *Intertech should discontinue using the exit that allows read-only access to all data that is not secured by rules.*

4. Documentation of key components of the ACF2 security infrastructure is inadequate.

Intertech prepares very little written documentation for the ACF2 security infrastructure. This makes identifying the purpose of and technical contact for specific security rules quite difficult. It also makes it difficult to scrutinize the appropriateness of rules. For example, during our audit, we found some security rules that granted access to every mainframe account. Security officers told us that they could not answer our questions about the propriety of these rules without first doing an extensive amount of research to identify what the rule was intended to protect. Other

information system professionals at Intertech were also unable to explain why these rules were needed.

Intertech has a very complex security infrastructure that contains over 60,000 ACF2 security rules. Without written documentation, challenging the appropriateness of individual security rules becomes extremely laborious. Inadequate documentation also could increase the time needed to recover business operations from a disaster.

Recommendation

- *Intertech and state agency security officers should develop written documentation for the ACF2 security infrastructure to facilitate security administration duties.*

Admin MINNESOTA Department of Administration

Office of the Commissioner
50 Sherburne Avenue
200 Administration Bldg.
Voice: 651.296.1424
Fax: 651.297.7909

October 9, 2000

James R. Nobles, Legislative Auditor
Room 140 Centennial Building
658 Cedar Street
St. Paul, MN 55155

Dear Mr. Nobles:

Thank you for meeting with us to review the results of the statewide information security audit of the ACF2 security software used at the InterTechnologies Group (ITG) of the Department of Administration. Your audit scope was a review of system-wide access to mainframe data stored at ITG as of June 2000 in order to identify and recommend areas needing improvement and/or correction.

This letter is to advise you that we are committed to implementing the recommendations you suggested in your Office of Legislative Auditor Report dated June 22, 2000.

Attached is a table summation of your findings, our planned corrective actions, the expected completion date of those projects, and the internal and external groups required to be involved in the completion of the improvements/corrective actions. The primary people responsible for delivery of these projects are Ray Kermode, Security Services Manager and Greg Dzieweczynski, Director, Interagency Services Division, InterTechnologies Group. They will issue quarterly reports beginning in January 2001 as to the progress of the planned improvements/corrective actions.

If you have any questions now or later, please do not hesitate to contact the InterTechnologies staff.

Very truly yours,

/s/ David Fisher

David Fisher
Commissioner

Attachment

cc: Jack Yarbrough

JULY 2000 LEGISLATIVE
AUDIT FINDINGS AND PLANNED CORRECTIVE ACTION

AUDIT FINDINGS	RISK	CORRECTIVE ACTIONS	EXPECTED COMPLETION DATE	INTERNAL AND EXTERNAL INVOLVMENT
FINDING 1) ACF2 rules give many InterTech employees and installed software product accounts widespread access to data.	Med.	Review InterTech's Technical Support staff and Software accounts to further limit access by specific job functions.	June 2001	ITG Tech Support
	Med.	Limit use of authorized programs to accounts needing access to perform their job functions.	June 2002 High risk pgms May 2001 Med. risk pgms Dec 2001 Low risk pgms June 2002	ITG Tech Support
FINDING 2) InterTech did not adequately control some powerful ACF2 privileges.	High	Review accounts with special ACF2 privileges and remove the privileges that give excessive access.	December 2000	ITG Tech Support Agency Security Staff
	High	Apply compensating controls to accounts that do not require passwords.	January 2001	ITG Tech Support Agency Security Staff Agency Developers
FINDING 3) One ACF2 exit may expose data to unauthorized access.	Low	Review need for exit by InterTech and other State agencies. If not needed, eliminate exit.	December 2001 Review March 2001 Update rules November 2001 Eliminate December 2001	ITG Tech Support ITG Application Support Agency Security Staff Agency Developers
FINDING4) Documentation of key components of the ACF2 security infrastructure is inadequate.	Low	Review and update security documentation.	December 2001 Agency rules February 2001 Internal rules May 2001 Software rules Dec 2001	ITG Tech Support ITG Application Support Agency Security Staff Agency Developers