OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial-Related Audit

Department of Administration
InterTechnologies Group
System-wide Access to Mainframe Data Follow-up

MAY 2, 2002 **02-26**

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

Senator Ann H. Rest, Chair
Legislative Audit Commission

Members of the Legislative Audit Commission

Mr. David Fisher, Commissioner
Department of Administration

We have conducted an information technology audit of select activities at the Department of Administration's InterTechnologies Group. The purpose of this audit was to follow-up on the prior audit issues identified in report 00-49, *System-wide Access to Mainframe Data*, released in October 2000. Our audit scope included a review of the corrective actions that the department had implemented as of January 2002.

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 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 complying 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 May 2, 2002.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen, CPA

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: January 31, 2002

Report Signed On: April 29, 2002

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 Follow-up

Table of Contents

Audit Participation

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

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Christopher Buse, CPA, CISA, CISSP	Information Technology Audit Manager
Mark Mathison, CPA, CISA	Auditor-in-Charge
Neal Dawson	Auditor
Eric Wion, CPA, CISA	Auditor

Exit Conference

We discussed the results of the audit with the following staff of the Department of Administration at an exit conference on April 12, 2002:

David Fisher	Commissioner
Kirsten Cecil	Deputy Commissioner
Larry Freund	Financial Managment Director
Deborah Tomczyk	Human Resources Director
Judy Hunt	Internal Audit Director
Jack Yarbrough	Assistant Commissioner, InterTechnololgies Group
Greg Dzieweczynski	Interagency Services Division Director, InterTechnologies Group
Ray Kermode	Security Services Manager, InterTechnologies Group

Department of Administration
InterTechnologies Group
System-wide Access to Mainframe Data Follow-up

Report Summary

The Department of Administration's InterTechnologies Group (InterTech) has made substantial progress in addressing the security weaknesses that we identified in our prior audit of system-wide access to mainframe data. However, none of the six recommendations in that report have been fully completed, and some security weaknesses still exist.

To improve controls, InterTech needs to continue working to fully complete the six recommendations that were in our prior report:

- 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.
- 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.
- InterTech should discontinue using the exit that allows read-only access to all data that is not secured by rules.
- InterTech and state agency security officers should develop written documentation for the ACF2 security infrastructure to facilitate security administration duties.

Chapter 1. Introduction

In October 2000, the Office of the Legislative Auditor issued report 00-49**,** *System-wide Access to Mainframe Data*. In that report, we concluded that 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, we found that an excessive number of these information system professionals and software products either had widespread access to data or could obtain this level of clearance through weaknesses in the security infrastructure.

The four findings in the report discussed shortcomings in the deployment and documentation of the state's ACF2 security infrastructure:

- ACF2 security rules gave many InterTech employees and installed software products widespread access to data.
- InterTech did not adequately control some powerful ACF2 privileges.
- One ACF2 exit exposed data to unauthorized access.
- Documentation of key components of the ACF2 security infrastructure was inadequate.

InterTech's management concurred with our findings and put forth a corrective action plan that addressed the six recommendations in the report. This plan included dates when specific corrective actions would be completed, ranging from January 2001 through June 2002. InterTech also provided quarterly status updates of this corrective action plan to the Legislative Auditor, the Commissioner of Finance, and the Governor. In its December 2001 update, InterTech indicated that it had completed four of the six audit recommendations. InterTech also stated that it planned to implement one of the remaining recommendations by June 2002 and the final recommendation during the next major release of ACF2.

The purpose of this audit is to evaluate the adequacy of the corrective actions taken by InterTech. Chapter 2 describes the scope of our work and the conclusions that we reached.

Chapter 2. Status of Prior Audit Recommendations

Chapter Conclusions

The Department of Administration's InterTechnologies Group has made substantial progress in addressing the security weaknesses that we identified in our prior audit report. However, in December 2001, InterTech reported to the Legislative Auditor, the Department of Finance, and the Governor that it had completed four recommendations and partially completed one. InterTech also indicated that it was waiting to address the final recommendation until the next major release of ACF2, the mainframe security software. We do not concur with those reported completion statuses. We found that the four recommendations that were classified as completed were only partially completed, and some security weaknesses still exist.

In our prior audit report, we concluded that ACF2 security rules gave large groups of InterTech employees and installed software products unnecessarily broad access to data. The report discussed many powerful accounts used by employees and software products that were not properly controlled. It also described how an ACF2 exit that was deployed by InterTech could lead to the inappropriate disclosure of sensitive data. Finally, the report discussed security infrastructure documentation shortcomings that came to our attention.

Audit Objective and Methodology

In this follow-up audit, we designed our work to answer the following question:

- Has InterTech taken appropriate actions to address the security weaknesses that we identified in our prior audit report?

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

Conclusions

InterTech has made substantial progress addressing the security weaknesses that we identified in our prior audit report. However, none of the six recommendations in the prior report have been fully completed.

In December 2001, InterTech reported to the Legislative Auditor, the Department of Finance, and the Governor that it had completed four of the six recommendations that were cited in our last audit report. We do not concur with those reported statuses. Table 2-1 illustrates the status of each audit recommendation that InterTech reported in December 2001. It also depicts our analysis of completion status, based on the work done during this follow-up audit.

Table 2-1
Completion Status of Prior Audit Recommendations
As of February 2002

Audit Recommendation	Status Reported By InterTech in December 2001 [1]	Status Confirmed During our Follow-up Audit Work [2]
InterTech should define ACF2 security groups that are appropriate for specific job functions.	Completed	Partially Completed
InterTech should evaluate the need for powerful group clearances permitted in ACF2 security rules.	Partially Completed	Partially Completed
InterTech should deploy the ACF2 recommended compensating controls over all accounts that do not require passwords.	Completed	Partially Completed
InterTech should remove powerful ACF2 privileges from those people who do not need those privileges.	Completed	Partially Completed
InterTech should discontinue using the exit that allows read-only access to all data that is not secured by rules.	Not Completed	Not Completed
InterTech and state agency security officers should develop written documentation for the ACF2 security infrastructure to facilitate security administration duties.	Completed	Partially Completed

Sources: [1] Department of Administration's Status Report on Resolving Findings in OLA Report 00-49, dated December 20, 2001.
[2] Conclusions from our follow-up audit work at InterTech during January 2002.

The following section displays the findings and recommendations that were communicated to the Department of Administration in our October 2000 report. It indicates the completion status of each recommendation that was reported by the Department of Administration to our office, the Commissioner of Finance, and the Governor. It also depicts our assessment of those completion statuses, based upon our follow-up audit work.

Department of Administration
InterTechnologies Group
System-wide Access to Mainframe Data Follow-up

Status of Prior Audit Findings and Recommendations

Prior Finding 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

- *Recommendation 1: InterTech should define ACF2 security groups that are appropriate for specific job functions.*

Implementation status reported by InterTech: COMPLETED

Follow-up audit assessment: PARTIALLY COMPLETEDD

InterTech reduced the membership in its most powerful ACF2 security groups. These reductions have limited the number of information technology professionals with unnecessary system-wide access to critical business data. However, InterTech has not assessed the appropriateness of software products that still retain their membership in these powerful security groups.

- *Recommendation 2: InterTech should evaluate the need for powerful group clearances permitted in ACF2 security rules.*

Implementation status reported by InterTech: PARTIALLY COMPLETED

Follow-up audit assessment: PARTIALLY COMPLETED

InterTech modified some ACF2 rules so that they no longer provide entire groups of people and software products with access to sensitive business data. Of greatest significance, InterTech now prohibits broad security groups from accessing critical programs and data that are part of the mainframe computer's operating system. However, we still identified other ACF2 rules that provided overly broad access to large groups of people and software products that InterTech needs to review.

Prior Finding 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

- *Recommendation 3: InterTech should deploy the ACF2 recommended compensating controls over all accounts that do not require passwords.*

Implementation status reported by InterTech: COMPLETED

Follow-up audit assessment: PARTIALLY COMPLETED

Our follow-up audit revealed extremely powerful accounts that were not appropriately protected. Although InterTech has reduced the number of these accounts, their existence still exposes mainframe data and computer resources to significant risk. InterTech should periodically review all privileged accounts that do not require passwords.

- *Recommendation 4: InterTech should remove powerful ACF2 privileges from those people who do not need those privileges.*

Implementation status reported by InterTech: COMPLETED

Follow-up audit assessment: PARTIALLY COMPLETED

Our follow-up audit found many people and software products that still had unnecessary ACF2 privileges. For example, in our October 2000 audit, we cited one employee who had an ACF2 privilege that gave him the ability to create and modify user accounts. This same employee still had this powerful privilege, even though his job duties do not include performing ACF2 security functions. InterTech has now removed this powerful privilege. Though InterTech corrected many of the specific issues identified in our October 2000 audit, it still has not developed a process to periodically recertify all accounts with powerful ACF2 privileges.

Prior Finding 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

- *Recommendation 5: InterTech should discontinue using the exit that allows read-only access to all data that is not secured by rules.*

Implementation status reported by InterTech: NOT COMPLETED

Follow-up audit assessment: NOT COMPLETED

In its December 2001 report, InterTech stated that it planned to eliminate this exit during the next major release of ACF2, most likely in the third quarter of 2002. Until that time, we encourage InterTech to communicate to its mainframe customers that any data stored under their personal accounts could be read by other people with mainframe accounts. InterTech does not write ACF2 security rules to protect data stored under customers' personal accounts. When no such rules exist, the exit deployed by InterTech provides all users with read access by default. ACF2 logs these type of accesses, making after the fact detection of inappropriate activity possible.

Prior Finding 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

- *Recommendation 6: InterTech and state agency security officers should develop written documentation for the ACF2 security infrastructure to facilitate security administration duties.*

Implementation status reported by InterTech: COMPLETED

Follow-up audit assessment: PARTIALLY COMPLETED

InterTech believes that the primary responsibility for security documentation rests with the state agencies that own the business applications and data that reside on the mainframe. With this in mind, InterTech undertook a project to document the purpose of every ACF2 security rule and to identify a technical contact name. However, at the time of our follow-up audit, InterTech had been able to acquire only 46 percent of the ACF2 rule information. While this information does not impact the operation of ACF2, it is vital to the long-term maintenance of the state's security infrastructure.

We concur that data owners are frequently in the best position to document their own security infrastructure. However, we question whether many small and mid-sized state agencies have the necessary technical skills to understand and document how ACF2 is used to secure their systems and data. Currently, InterTech security officers write ACF2 rules on behalf of most small and mid-sized agencies. While these concerns extend beyond the scope of our current audit, we believe they may warrant further study in the future.

Admin MINNESOTA
Department of Administration

Office of the Commissioner
200 Administration Building
50 Sherburne Avenue
St. Paul, MN 55155
Telephone: 651.296.1424
Fax: 651.297.7909
TTY: 651.297.4357

April 24, 2002

James R. Nobles, Legislative Auditor
First Floor South, Centennial Building
658 Cedar Street
St. Paul, MN 55155

Dear Mr. Nobles:

InterTechnologies Group (ITG) staff has reviewed the prior audit issues contained in the Office of the Legislative Auditor (OLA) Report 00-49, *System-wide Access to Mainframe Data*.

We concur with the OLA's conclusions in the recent follow-up audit draft that we have made significant progress in addressing security weaknesses, and we are continuing efforts to strengthen mainframe security controls. Over the past sixteen months the five-person Mainframe Security Function (MSF) Unit at ITG has been reviewing, starting with those with the highest risk exposure, the 60,000+ access privileges contained in the MSF's ACF2 Security System. This review has resulted in significant improvements in the MSF, as was acknowledged in the OLA's April 11, 2002, draft follow-up audit report, including the establishment of new access groupings, and the elimination or restriction of inappropriate and unnecessary access privileges.

MSF has evolved over the years (the ACF2 Security Software was installed in 1980) and continues to evolve today. Even though there has been substantial progress, we all recognize that computer security, particularly the MSF, is a "journey and not a destination"; i.e., there will always be changes in staff and software that will necessitate ongoing and annual access privilege reviews and changes.

To address the OLA's concerns and to ensure that the MSF continues to protect state data, the ITG MSF Unit, managed by Ray Kermode and staffed with four computer security professionals, has:

1) Developed a step-by-step procedure to review all ACF2 authorized accesses for appropriateness and necessity, and to de-activate or limit any determined to be inappropriate and/or unnecessary. Those determined to be appropriate and necessary will be "certified" as being acceptable. This review process was started in April 2002 and will be completed in July 2002.

2) While conducting the above review (see #1), the MSF Unit is identifying a contact ("owner") for each authorized access and recording this access in the ACF2 database. Concurrently, the MSF Unit is working with state agency security officers to develop written documentation providing guidance, as necessary, in describing each ACF2 access authorization. The deadline for completion is September 2002.
3) The MSF Unit is developing an ongoing review and annual re-certification process for all ACF2 access authorizations to ensure that all privileged accesses that have been previously "certified" remain appropriate and necessary, and that the documentation remains current. The deadline for completion is July 2002.
4) We are also developing plans for the installation of the latest version of ACF2 that permits elimination of exits allowing read-only access to the data on the mainframe that does not have ACF2 rules. The vendor has already released the necessary version and we plan to install it in July of 2002. Following installation, all uses of this exit require review and where appropriate and necessary, they will be eliminated. All reviews are to be completed by September 2002.

Major considerations/guidelines for the MSF Unit in performing the above tasks are:

- Ensuring that all access authorities are both appropriate and necessary for overall security and operational requirements.
- Continuing to review access groupings that are appropriate for specific operational processing and job functions to ensure that the required controls can be implemented and managed.
- Determining appropriate deployment/use of ACF2 compensating controls over all accesses that do not require passwords.

In closing, ITG wishes to thank the OLA for conducting this review and for their assistance in identifying potential system vulnerabilities. Our plan is to work closely with the OLA as we continue the "security journey." It is also our plan that the MSF Unit will issue quarterly reports on its progress to the OLA, the Department of Finance, and the Office of the Governor.

Very truly yours,

/s/ David F. Fisher

David F. Fisher
Commissioner