O L A **OFFICE OF THE LEGISLATIVE AUDITOR**
STATE OF MINNESOTA

Financial Audit Division Report

Minnesota Office of Enterprise Technology

Mainframe Security Audit
As of October 2005

DECEMBER 7, 2005 **05-55**

Financial Audit Division

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

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

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

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

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

Through its Program Evaluation Division, OLA conducts several evaluations each year.

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

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

This document can be made available in alternative formats, such as large print, Braille, or audio tape, by calling 651-296-1235 (voice), or the Minnesota Relay Service at 651-297-5353 or 1-800-627-3529.

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

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

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. Gopal Khanna, Chief Information Officer
Minnesota Office of Enterprise Technology

We have conducted an information technology audit of security controls established to protect the integrity and confidentiality of data stored on the state's mainframe computers. The Office of Enterprise Technology is responsible for managing these computers. Part of this responsibility includes the establishment of security measures to protect sensitive government data and computer resources. Our audit assessed the adequacy of mainframe security controls as of October 2005. The Report Summary highlights our overall conclusions. Our specific audit objectives and conclusions are contained in Chapter 2 of this report.

This audit identified serious security weaknesses that exposed government data to an unacceptable risk of loss, misuse, or disclosure.

We would like to thank staff from the Office of Enterprise Technology for their cooperation during this audit.

/s/ James R. Nobles	*/s/ Claudia J. Gudvangen*
James R. Nobles Legislative Auditor	Claudia J. Gudvangen, CPA Deputy Legislative Auditor

End of Fieldwork: October 21, 2005

Report Signed On: December 5, 2005

Minnesota Office of Enterprise Technology
Mainframe Security Audit

Table of Contents

Audit Participation

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

Claudia Gudvangen, CPA	Deputy Legislative Auditor
Chris Buse, CPA, CISA, CISSP	Information Technology Audit Manager
Mark Mathison, CPA, CISA	Auditor-in-Charge
Eric Wion, CPA, CISA, CISSP	Auditor
John Kelcher	Auditor

Exit Conference

We discussed the findings and recommendations in this report with the following staff of the Minnesota Office of Enterprise Technology on November 23, 2005:

Gopal Khanna	Chief Information Officer
Steve Stedman	Chief Technology Officer
Jack Yarbrough	Director of Shared Services
Greg Dzieweczynski	Director of Interagency Services
Jim Steinwand	Security Services Manager

Minnesota Office of Enterprise Technology
Mainframe Security Audit

Report Summary

Conclusion:

Even though the Office of Enterprise Technology deployed multiple layers of security, data stored on the state's central mainframe computers was still vulnerable to loss, tampering, and unauthorized disclosure.

Key Findings:

- The Office of Enterprise Technology does not have a comprehensive security program to address pertinent technology risks. (Finding 1, page 5)
- Access to mainframe computer programs and data was not adequately restricted. (Finding 2, page 7)
- Unauthorized changes to critical system files could occur and could go undetected. (Finding 6, page 11)

The audit report contained eight audit findings relating to internal control over the Office of Enterprise Technology's mainframe computing environment.

Audit Scope:

Audit Period:
As of October 2005

Audit Scope:
Security controls designed to protect the integrity and confidentiality of data stored on the state's mainframe computers

Background:

The Office of Enterprise Technology (OET) is responsible for managing the central mainframe computing facility, which houses some of the state's most important business systems and data. The complexity of the mainframe environment makes it difficult to secure. Thousands of software products run on the mainframe computers, any of which could affect security.

The 2005 Legislature created OET to provide technology leadership and oversight for state government. The new agency began operations on July 1, 2005, assuming the staff and resources of the Minnesota Office of Technology and the InterTechnologies Group, both former divisions of the Department of Administration. The Legislature placed OET under the direction of a Chief Information Officer, a cabinet-level position appointed by the Governor.

Chapter 1. Introduction

This audit assessed the adequacy of controls designed to protect the integrity and confidentiality of data stored on the state's mainframe computers.

The Office of Enterprise Technology (OET) is now responsible for managing the central mainframe computing facility. The 2005 Legislature created OET to provide technology leadership and oversight for state government. The new agency began operations on July 1, 2005, assuming the staff and resources of the Minnesota Office of Technology and the InterTechnologies Group, both former divisions of the Department of Administration. The Legislature placed OET under the direction of a Chief Information Officer, a cabinet-level position appointed by the Governor. On August 15, 2005, Governor Tim Pawlenty appointed Gopal Khanna to serve as the first Chief Information Officer for the State of Minnesota.

The mainframe computers 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;
- licensing drivers and motor vehicles;
- processing payments to vendors and maintaining accounting records; and
- paying the state's workforce

The OET uses multiple layers of security to protect these business systems and data. For example, OET uses security tools to control network connections to its mainframe computers. OET also restricts physical access to the mainframe computing facility. One of the most important security layers is an access control software package called ACF2, which 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 OET have primary responsibility for administering ACF2. However, OET delegates some of its security administration duties to security officers who work for several of the largest state agencies. Together, OET and these agency security officers manage thousands of ACF2 security rules, as well as accounts that have clearance to access mainframe data. OET and agency security officers created many of these accounts for employees that need to interact with specific business systems. Software products installed on the mainframes use the remaining accounts.

In 2000, our office conducted an audit that assessed the adequacy of selected mainframe security controls. That audit included many of the same areas that we reviewed during this audit. In our October 2000 report, we concluded that an excessive number of people either had widespread access to data or could obtain that level of clearance through weaknesses in the security infrastructure. The report contained four findings and six recommendations that addressed a broad array of security issues. Many of the issues cited by our audit also were included in a June 1999 report, written by a consulting firm engaged by the InterTechnologies Group.

In December 2001, the InterTechnologies Group reported to our office, the Department of Finance, and the Governor that it had completed four and partially completed one of the six recommendations in our October 2000 report. In May 2002, we conducted a follow-up audit and concluded that we did not concur with the reported completion status. We found that the four recommendations classified as completed were only partially completed, and security weaknesses still existed. However, we noted that the InterTechnologies Group had made progress in addressing the security weaknesses in our October 2000 report.

Audit Approach

We conducted our audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we obtain an understanding of internal controls that are relevant to the audit objectives. *Government Auditing Standards* also require that we plan our work to provide reasonable assurance that the agency complied with financial-related legal provisions that are significant to the audit. In determining the agency’s compliance with legal provisions, we considered requirements of laws, regulations, contracts, and grant agreements.

OET had few documented policies, procedures, and standards for its mainframe environment, causing us to place extensive reliance on external sources for evaluation criteria. To assess the adequacy of controls, we obtained criteria from the *Control Objectives for Information and Related Technology* (COBIT). Published by the IT Governance Institute, COBIT includes 34 high-level control objectives and 318 detailed control objectives, grouped in four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring. We also used mainframe security standards developed by the United States Defense Information Systems Agency for the Department of Defense and published in the *OS/390 & z/OS Security Technical Implementation Guide*. Finally, we obtained evaluation criteria from information published by the developers of products installed on the mainframe, such as ACF2.

This information technology audit included a review of security data that the Minnesota Data Practices Act classifies as nonpublic. To protect state resources and comply with the Minnesota Data Practices Act, we withheld specific security-related details from this publicly released report. We communicated the pertinent details to OET administration in a separate, nonpublic document.

Chapter 2. Mainframe Security Controls

Chapter Conclusions

Even though the Office of Enterprise Technology deployed multiple layers of security, data stored on the state's mainframe computers was still vulnerable to loss, tampering, and unauthorized disclosure. Of particular concern, our audit identified security weaknesses from prior audits that management did not adequately address.

This information technology audit is another in a series of audits done by our office that focused on mainframe security. We spend a significant portion of our technical audit resources on the mainframe environment because state government could not function without it. From collecting taxes to administering social service programs, state agencies depend on the continuous availability of the central mainframe computers. We also concentrate on this environment because it houses enormous quantities of data. Protecting the integrity and confidentiality of this data is vital to both state government and the citizens that it serves.

The complexity of the mainframe environment makes it difficult to secure. Thousands of software products run on the mainframe computers, any of which could affect security. Furthermore, thousands of employees and business partners need access to fulfill their job duties. Adding to this complexity, many connections to the mainframe computers now occur over the Internet. In fact, some state agencies now use the mainframe computers to host their web-based computer applications.

Audit Objective

We designed our audit work to answer the following question:

- Did the Office of Enterprise Technology (OET) design and implement appropriate controls to protect the integrity and confidentiality of mainframe data?

To answer this question, we interviewed information technology professionals and reviewed documentation to gain an understanding of controls. We also used computer assisted audit tools to gather and analyze mainframe security data.

Though we addressed our objectives and conclusions to OET, it is important to note that the Department of Administration managed the state's mainframe computers until June 30, 2005.

Current Findings and Recommendations

1. The Office of Enterprise Technology does not have a comprehensive security program to address pertinent technology risks.

The number, type, and pervasiveness of issues in this and prior audits indicate that there are serious problems with the mainframe security program. We identified several factors that are contributing to its ineffectiveness:

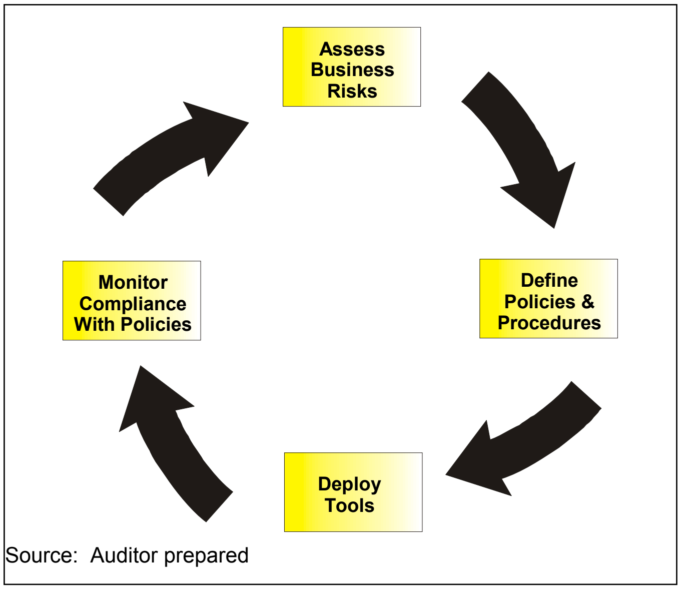
Unclear Authority and Responsibility

Management has not given any one group the authority and responsibility to develop a comprehensive security program. OET has a Security Services Unit, which spends most of its time managing ACF2 security rules and accounts. However, other operational groups throughout the organization perform tasks that affect mainframe security as well. In many cases, these groups make security decisions without consulting Security Services employees. Many of the detailed security weaknesses that we brought to management's attention resulted from decisions made by employees that were not part of Security Services.

Inadequate Resources

Management told us that the Security Services Unit is doing more with less, which is true. The unit now has fewer staff than it did during our last audit. Unfortunately, complex security issues often require staff to spend significant amounts of time doing research and testing. We question whether the current unit will have sufficient resources to remedy all of the outstanding audit issues and complete its daily security responsibilities.

Few Written Policies, Procedures, and Standards


Assess Business Risks
Define Policies & Procedures
Deploy Tools
Monitor Compliance With Policies

Source: Auditor prepared

We found few written policies, procedures, and standards in any of the areas that we audited. Policies, procedures, and standards are typically the products of a formal risk management process. They outline management's security expectations and methods to fulfill those expectations. Organizations typically begin this process by performing a detailed risk analysis to identify potential vulnerabilities. The results of this analysis help organizations design policies, procedures, and standards to reduce their exposures to a level that executive management is willing to accept. Security professionals then deploy tools, such as access control software, to enforce the standards sanctioned by management. Information provided by these tools helps organizations monitor compliance and fine-tune subsequent risk assessments in the ongoing security management lifecycle.

Absent written guidelines, Security Services employees had difficulty providing us with answers to basic security questions, such as:

- What are the criteria for granting people or groups different types of extremely powerful or system-wide security clearances?

- What mitigating controls did management require to ensure that people or groups did not abuse extremely powerful security clearances?

- Who has authority to make decisions that affect mainframe security, and what is the scope of their authority?

Security professionals cannot make consistent decisions without standards to refer to as guidance. Had it proactively defined and communicated its security expectations, we think that management may have averted many of the findings in this report.

In its broadest sense, a security program is nothing more than formal ways to manage risk. Management only has two choices: either accept or mitigate the threats that it faces. However, making informed decisions requires ongoing assessments of operations to determine what can go wrong. In its June 1999 report, a consulting firm told the InterTechnologies Group that it was in an undesirable position of accepting risk without understanding what those risks were. Our audit results confirm that OET is still in that same undesirable situation today because it does not do enough proactive security planning.

Recommendations

- *The Office of Enterprise Technology should give some person or group the authority and responsibility to develop and implement a comprehensive security program.*

- *The person or group in charge of the security program should be provided sufficient resources to:*

  - *lead organization-wide risk assessment efforts;*
  - *coordinate the development and dissemination of policies, procedures, and standards;*
  - *ensure that security tools are properly configured; and*
  - *monitor compliance with policies, procedures, and standards.*

2. Access to mainframe computer programs and data was not adequately restricted.

Our audit identified many people and software products with security clearances that provided much broader access than necessary. In some cases, security weaknesses exposed mainframe data to an unnecessary risk of loss, tampering, or unauthorized disclosure. Other weaknesses could have resulted in disruptions to critical mainframe services. The following sections discuss some of the most significant security weaknesses that we brought to management's attention. In the short-term, OET needs to remedy the specific security weaknesses identified by our audit. Implementing the recommendations discussed in Finding 1 will help the organization manage security more proactively and avoid similar issues in the future.

Weak Controls Over Computer Programs That Can Bypass Security

By design, some mainframe computer programs have the ability to circumvent security. Access to these high-risk programs and the special libraries where they reside should be limited to select individuals who need clearance to fulfill their job duties. Furthermore, most experts agree that any modifications to these programs should take place through a regimented change management process with well-defined checks and balances. Without strong security and change control procedures, unscrupulous individuals could alter and use these programs to steal data or perform mischievous acts.

Our audit identified between 65 and 224 accounts with the ability to update these types of high-risk programs, stored in over 400 libraries. In our opinion, many of these accounts did not need this clearance. We also found two libraries that had weak security settings, giving any person with mainframe access the ability to make unauthorized program changes.

Finally, as discussed in Finding 6, OET did not deploy robust change management procedures or consistently log modifications to these high-risk programs. As a result, unauthorized changes could occur and could go undetected.

Unsecured Tape Management Utility Programs

State agencies store vast quantities of data on magnetic tape. Using improperly secured utility programs, unauthorized persons could have viewed, modified, or deleted any tape data in the mainframe environment. Typically, only information technology professionals who manage tape libraries need clearance to use these types of powerful utility programs. At the time of our audit, approximately 4,100 people and software products had this clearance.

Poorly Written Security Rules

ACF2 security software provides robust protection by default. In fact, ACF2 will not permit a person or an installed software product to access data or use any mainframe computer resource unless a security rule explicitly authorizes that action. However, we identified many poorly written ACF2 security rules. Some of these rules gave large groups of people or everyone on the mainframe inappropriate clearance to read data, while others provided clearance to change or delete data. We analyzed some of the files at risk and found extremely sensitive information, such as citizens' credit card numbers and personal information. We also found accounts and passwords for other state agency computers that interact with the mainframe. Using that information, we were able to access a computer owned by another state agency.

Inadequate Controls Over Accounts Without Passwords

By design, some accounts with access to the mainframe computers do not have passwords. Fortunately, ACF2 provides a number of compensating controls to prevent inappropriate use of these accounts. Organizations that fail to deploy these controls expose mainframe data and computer resources to extreme risk.

In our 2000 audit, we identified many mainframe accounts without passwords or other compensating controls. Since our last audit, OET applied compensating controls to most of these accounts. However, we still found over 200 accounts without passwords that were susceptible to abuse.

Excessive Access to Powerful Commands

Information technology professionals use operating system commands to perform extremely sensitive functions, such as starting and stopping the mainframes. They also issue powerful commands to administer core software products that run on the mainframes, such as ACF2. Commands can pose extreme risks if not properly controlled. Therefore, organizations must limit the ability to issue certain commands to specific individuals who need that capability.

We found weaknesses in the ACF2 security rules that define who can issue certain powerful commands. Of greatest significance, security rules gave virtually all people with mainframe clearance the ability to issue some commands that could impact system functionality or reveal security information. These security weaknesses resulted in one instance where an employee at another state agency erroneously issued a sensitive command that disrupted mainframe computer processing for a short period.

Database Security Information Was Not Adequately Controlled

Due to weak security settings, people with access to some mainframe databases could obtain nonpublic security data. Database security information should only be accessible to system administrators and security professionals. The inappropriate security settings that we found gave people the means to identify all accounts with access to the databases as well as the security permissions assigned to each account.

Recommendation

- *The Office of Enterprise Technology should fix the specific issues that we brought to its attention by adjusting security clearances to only give people and software products the minimum clearance necessary.*

3. Unsecured methods can be used to connect to the mainframe computers.

The mainframe computers let people establish and do work over unencrypted connections. Unencrypted connections are risky because account names, passwords, and other types of nonpublic data can flow over public networks in a human readable form. Encryption is an important control because it makes data unreadable to people who intercept network transmissions for unauthorized purposes.

Recommendation

- *The Office of Enterprise Technology should replace unsecured connection methods with those that use encryption.*

4. Some unneeded mainframe accounts were not disabled or removed.

Security professionals in OET and some large state agencies did not promptly remove or disable unneeded mainframe accounts. Inactivating unnecessary accounts is a key control to prevent former employees or other unauthorized persons from accessing the mainframes. The Security Services Unit developed processes to identify and inactivate accounts. However, some inactive accounts were not identified because of flaws in the unit's procedures. We found over 50 accounts that belonged to people who left state service or were on extended leaves of absence. We also found over 900 accounts assigned to software products that security officers did not remove or disable. All of these software accounts were inactive for at least one year, and some had been inactive for over ten.

Recommendation

- *The Office of Enterprise Technology should develop procedures to promptly remove or disable unneeded accounts.*

5. Procedures to confirm the identity of people with access to the mainframe computers were weak in several respects.

OET relies on unique accounts and passwords to validate the identity of people with access to the mainframes. Commonly referred to as single factor authentication, this approach places complete reliance on a secret password, known only by one person. Organizations that use single factor authentication need controls to ensure that passwords are extremely difficult to guess. Without strong password controls, hackers and other unscrupulous individuals can assume the identity of legitimate system users to gain unauthorized access. We reported many detailed password-related weaknesses to management. However, described below are two particularly significant issues that came to our attention.

Static Passwords Allowed

Security officers configured many software program accounts so that ACF2 did not enforce periodic password changes. They did this to prevent mission critical tasks from failing due to expired passwords. However, organizations that disable automated password change features must put in place their own controls to ensure that passwords to powerful accounts do not become widely known. Particularly with software accounts, an ever-increasing number of information technology professionals end up knowing passwords as time passes.

We found many accounts with very old passwords. As a result, it is safe to assume that the passwords were known by people who no longer had a business need to access the accounts, including people who no longer work for the state. Two of the oldest passwords belonged to accounts that last had their passwords changed in 1982.

Default Passwords Not Changed

Many software products come with default user accounts and passwords. It is important to change default passwords because hackers frequently use them to gain unauthorized access. In fact, lists of default accounts and passwords for most software products are available on the Internet.

We found one mainframe software product with a default password that was not changed. With this account and password, we were able to obtain an extremely powerful security clearance that gave us very broad access to mainframe data.

Finally, we question the appropriateness of single-factor authentication for security officers and other information technology professionals with extremely powerful security clearances. Most security experts agree that passwords alone are a weak form of authentication. Supplementing secret passwords with additional controls, such as smart cards or biometric devices, would make it much more difficult for hackers to gain access to the most powerful accounts with system-wide access to data.

Recommendations

- *The Office of Enterprise Technology should regularly change passwords to software accounts.*

- *The Office of Enterprise Technology should change default passwords after installing software.*

- *The Office of Enterprise Technology should consider additional authentication controls for security officers and other information technology professionals with extremely powerful security clearances.*

6. Unauthorized changes to critical system files could occur and could go undetected.

OET does not have all the necessary controls to prevent or detect unauthorized changes to files that could affect mainframe security. We assessed controls over certain high-risk computer programs that have the ability to bypass security. We also examined controls over some security-related mainframe operating system files. This testing revealed numerous information technology professionals and software products with clearances to change critical files. OET installed a mainframe software product that can help organizations control changes to critical system files. However, OET was not using the product to manage changes to most of the files that we tested.

To improve controls, OET needs to develop procedures to manage changes to critical files. These procedures should ensure that no individual has clearance to make critical system changes without independent oversight. They also should outline stringent documentation and testing requirements.

Recommendation

- *The Office of Enterprise Technology should develop controls to ensure that changes to critical mainframe programs go through a formal change management process.*

7. The Office of Enterprise Technology does not have a comprehensive security monitoring strategy.

OET lacked important controls to detect and quickly respond to security-related events, such as intrusion attempts or data modifications made by unauthorized people. We found that OET did not do a thorough job of defining what security events must be monitored. In addition, the agency did not identify who was responsible for performing some types of monitoring activities.

As discussed in Finding 1, OET has few security-related policies, procedures, and standards. Without standards, security professionals have had difficulty determining what monitoring data is most important to gather. For data that is currently gathered, security professionals have difficulty identifying anomalies because OET has few baseline standards to use as measurement criteria. To illustrate, employees in the Security Services Unit get a series of standard ACF2 security reports each day. Though they reviewed these reports, in many cases the process added little value because the security officers did not understand which items in the reports were exceptions.

For software products other than ACF2, it was not clear who was responsible for monitoring security events or if events were monitored at all. We found one security weakness that let us use one of the most powerful mainframe accounts. No employee recognized that we were able to gain this elevated level of security clearance until we notified management.

Recommendation

- *The Office of Enterprise Technology should develop a comprehensive strategy for monitoring security-related events.*

8. Physical access to the data center was not properly controlled.

The state's central data center houses mission critical computer equipment. To protect this sensitive equipment, access to the center must be restricted to only those people who need clearance to fulfill their job duties. Approximately 300 people had key cards that provided access to the data center. While most were OET staff, many did not need this level of security clearance.

The data center also houses computer equipment that belongs to other state agencies. Currently, physical barriers are not in place to keep employees from other agencies away from the mainframes and other OET computers. As more agencies move their equipment to the central data center, OET may need to explore additional physical access controls.

Recommendation

- *The Office of Enterprise Technology should limit access to the data center to only those people who need access to perform their job duties.*

Status of Prior Audit Issues
As of October 21, 2005

Most Recent Audit

Legislative Audit Report 02-26 was a follow-up audit to assess the status of various security weaknesses identified during a previous information technology audit, publicly released October 19, 2000, that focused on selected controls to help secure system-wide access to mainframe data. That report concluded that the agency had taken some steps to fix some of the weaknesses reported, but some security weaknesses still existed.

The scope of this audit included many of the same areas that we reviewed during 2000. Embedded in the findings of this report are references to prior audit issues that were not adequately addressed.

State of Minnesota Audit Follow-Up Process

The Department of Finance, on behalf of the Governor, maintains a quarterly process for following up on issues cited in financial audit reports issued by the Legislative Auditor. The process consists of an exchange of written correspondence that documents the status of audit findings. The follow-up process continues until Finance is satisfied that the issues have been resolved. It covers entities headed by gubernatorial appointees, including most state agencies, boards, commissions, and Minnesota Office of Enterprise Technology. It is not applied to audits of the University of Minnesota, any quasi-state organizations, such as metropolitan agencies or the State Agricultural Society, the state constitutional officers, or the judicial branch.

Office of Enterprise Technology

December 5, 2005

Mr. James R. Nobles
Legislative Auditor
Room 140 Centennial Building
658 Cedar Street
St. Paul, MN 55155-1603

Dear Mr. Nobles:

Thank you for the opportunity to review and respond to your office's audit of mainframe security at the Office of Enterprise Technology (OET). We appreciate the expertise and thoroughness displayed by your audit staff during the course of the audit.

While we may disagree with the magnitude of actual risk involved with some of the audit findings and recommendations at a detail level, we accept that the major thrust of the Office of Legislative Auditor report is on the whole an accurate assessment.

The report leaves one unfortunate and, I believe, misleading impression regarding our efforts to implement past recommendations. Contrary to the report, we have made substantial progress on many of the issues raised in previous audits. Although work remains in these areas because of resource limitations and evolving procedures, we have shared our plans and results with the OLA and continue to work on them. I know Commissioner Badgerow took the findings seriously and assure you we will increase our efforts to complete the work of making our environment secure, now and on an ongoing basis. As your office can attest, some of the detailed findings and issues identified during the course of both previous audits and the current audit have already been remedied. For previous audits, the OLA was kept involved in and informed about the remediation plan and the progress against that plan.

In any event, it's clear that not all of the planned improvements in conditions identified in previous audits have been implemented to your satisfaction, and that we haven't yet made an appropriate level of commitment to addressing the myriad administrative details of aggressive management of mainframe security. This is changing.

Similarly, our relatively minor disagreements with current OLA findings and recommendations should not be the basis for failure to reach agreement on proper approaches to problems and then act on those agreements. We are committed to maintaining a secure environment through a combination of sound security policies and rigorous administration of those policies.

As Mr. Buse noted in the report, the complexity of the mainframe environment is a complicating factor in security management; this, and the extent of involvement of so many stakeholders in routine operations, makes robust security both difficult and very necessary. The audit was directed at aspects of our environment that are the legitimate area for OET and agency staff involvement. The nature of this involvement and the nature of their jobs demand that significant authority must be granted for them to do their work.

To one degree or another, some conflict between security and authority to act is inevitable, even in the security community itself. The question of "who watches the watchers" has existed as long as control processes have been around. The point of the audit was that we need to do a better job establishing procedural safeguards, documentation and follow-up to govern the granting and administration of these authorities, even though the employees are screened, trained and supervised.

It's not enough to say that you found no evidence that security was breached from the outside, or that any damage was actually done to systems or data. Although the potential security issues raised in the audit were associated with people already within the system rather than people "in the wild" (which limits the practical exposure), the fact remains that luck isn't a sufficient strategy for prevention of violation, nor is administrative inconvenience an excuse for inaction.

Security is more than just a matter of technology, and the OLA audit properly points out our inadequacies in process and organization. When I arrived here three months ago, I immediately identified the many dimensions of security as one of our highest priorities. The audit appropriately draws attention to the needs in this area.

Before I respond to the specific findings and recommendations, I want you to know that I have directed the following actions to take place immediately to address the systemic issues and remedy the shortcomings of OET in this critical area:

- I will be appointing an executive-level Chief Information Security Officer for the state, with authority to build, implement, and maintain a robust security environment. The CISO will be independent of the operational side of our organization and shall have the responsibility for security policy and security administration for the enterprise.
- Policy changes and procedures will take time to develop and implement, and as was noted in the audit, resources and workload are major obstacles to complete implementation of security improvements. However, our obligation is to make the environment secure, and I will seek the financial, technological and human resources needed to implement changes in our procedures as recommended by the OLA. A detail plan for remediation, with timetables and responsibilities identified, will be developed in the very near future, and we will work with OLA to monitor its progress.
- I will incorporate into statewide strategic plans for information management specific long-term plans for maintaining a secure environment beyond the specific actions suggested by the audit.

With the changes in reporting and resources, I am confident that we will successfully address the shortcomings in our security and carry out our remediation strategies. We must be able to assure our clients and citizens that their data and their investments in our systems and networks are protected in an increasingly challenging and dangerous technology environment.

Once again, thank you for the work your office has done on behalf of the State, and for the opportunity afforded us to have a constructive discussion with you about the issues raised in the audit.

Sincerely,

/s/ Gopal K. Khanna

Gopal K. Khanna
State Chief Information Officer
Commissioner, Office of Enterprise Technology

Attachment
Specific Responses to
Findings and Recommendations

1. Finding: *The Office of Enterprise Technology does not have a comprehensive security program to address pertinent technology risks.*

Recommendations: The Office of Enterprise Technology should give some person or group the authority and responsibility to develop and implement a comprehensive security program.

The person or group in charge of the security program should be provided sufficient resources to:

- lead organization-wide risk assessment efforts;
- coordinate the development and dissemination of policies, procedures, and standards;
- ensure that security tools are properly configured; and
- monitor compliance with policies, procedures, and standards.

Response: We agree. The Commissioner of Enterprise Technology is planning to appoint a state Chief Information Security Officer, and OET is working with the state's security community to address the creation of an enterprise-wide comprehensive security program.

Internal to OET, the Security Services Unit and its current management have been given the necessary authority to cross interdepartmental lines to ensure that this unit can and will act decisively to: lead the organization-wide risk assessment efforts; coordinate the development and dissemination of policies, procedures and standards; ensure that security tools are properly configured; and monitor compliance with policies, procedures and standards. We are currently exploring what the necessary level of staffing resources should be for remedial and ongoing operations, as well as determining how to secure those resources.

2. Finding: *Access to mainframe computer programs and data was not adequately restricted.*

Recommendation: The Office of Enterprise Technology should fix the specific issues that we brought to its attention by adjusting security clearances to give people and software products only the minimum clearance necessary.

Response: We agree. The Security Services Unit has been working diligently to address the audit issues that relate to mainframe access, within the limits of current resources. We will address these access issues according to our evaluation of risk. Most of the individuals possessing such access rights need them to do their work and use their access authority with great discretion. For the small number of others identified by the OLA, we will work to achieve a greater degree of refinement in our access. However, in fairness to these individuals, all of them are considered trusted staff, have completed security background checks, including fingerprinting, prior to employment with OET, and are currently employed in positions where a level of access is required. These few are primarily the accounts addressed in this finding.

While addressing the Poorly Written Security Rule section of this finding, any and all credit card and personal information existed only in a temporary test file, which was immediately removed upon discovery, and the information does not exist anywhere on the mainframe system (to our knowledge). Also, a software flaw was discovered by the auditors and reported to the software vendor. This flaw allowed accounts and passwords from other agencies to be discovered, and affected all systems worldwide. The vendor immediately acknowledged the flaw and provided a fix for the software that removed the flaw. It is no longer possible to find accounts and passwords from other agencies on the system.

In response to the identification of over 200 accounts without passwords in another agency, OET has been working with that agency to remove those accounts entirely or put in place proper compensating controls over them. The number of such accounts has been reduced to 53 as of the date of this response.

The remaining issues presenting in this finding are in various stages of being addressed, remedied, and/or removed from the system by properly adjusting the security clearances given to people and software.

3. Finding: *Unsecured methods can be used to connect to the mainframe computers.*

Recommendation: The Office of Enterprise Technology should replace unsecured connection methods with those that use encryption.

Response: We agree. Policies, standards and procedures have been discussed for some time. Implementation plans are being developed and appropriate technologies are being investigated to remove the ability for anyone to send or receive unencrypted communications to the mainframe.

4. Finding: *Some unneeded mainframe accounts were not disabled or removed.*

Recommendation: The Office of Enterprise Technology should develop procedures to promptly remove or disable unneeded accounts.

Response: We agree. The Security Services Unit of OET recognizes, as does the Office of the Legislative Auditor, that other agencies must participate in the effort to promptly and properly remove or disable unneeded accounts. OET will work both internally and with the agencies to develop policies and procedures to remove unneeded accounts.

5. Finding: *Procedures to confirm the identity of people with access to the mainframe computers were weak in several respects.*

Recommendations:

- The Office of Enterprise Technology should regularly change passwords to software accounts.
- The Office of Enterprise Technology should change default passwords after installing software.

- The Office of Enterprise Technology should consider additional authentication controls for security officers and other information technology professionals with extremely powerful security clearances.

Response: We agree. OET will create policies and procedures to properly drive the changing of passwords to software accounts and the removal of default passwords after installing software. OET agrees that passwords alone, regardless of their strength, are often insufficient to properly protect valuable data and systems, and will begin the investigation of the use of two factor authentication (biometrics and tokens are an example of two factor authentication) for security officers and others with extremely powerful security clearances.

6. Finding: *Unauthorized changes to critical system files could occur and could go undetected.*

Recommendation: The Office of Enterprise Technology should develop controls to ensure that changes to critical mainframe programs go through a formal change-management process.

Response: We agree. On November 1, 2004, the Security Services Unit initiated an OET internal project to address the issues in this finding, but due largely to insufficient staffing, the project did not progress as quickly as hoped. OET did install software to assist in managing software and critical library changes, which primarily allowed the auditors to more fully discover our weaknesses. OET will again attempt to more fully utilize the installed software in the manner for which it was intended, and will revise and modify the current change control process to discover, prevent or detect unauthorized changes.

7. Finding: *The Office of Enterprise Technology does not have a comprehensive security monitoring strategy.*

Recommendation: The Office of Enterprise Technology should develop a comprehensive strategy for monitoring security-related events.

Response: We agree. OET will aggressively pursue the development and implementation of a comprehensive security monitoring strategy for ACF2 and other software products used in the mainframe environment

8. Finding: *Physical access to the data center was not properly controlled.*

Recommendation: The Office of Enterprise Technology should limit access to the data center to only those people who need access to perform their job duties.

Response: We agree. OET is already in the process of revising and implementing its data center physical access policy to limit access to only those people who need access to perform their job duties, and will make other changes as necessary to support this policy.

Admin
Minnesota
DEPARTMENT OF ADMINISTRATION

December 5, 2005

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

Dear Mr. Nobles:

Last week, I received a copy of the revised draft report containing the results of your office's recent information technology audit of security controls for data stored on the state's mainframe computers. This report acknowledges that the Department of Administration (Admin) managed the state's mainframe computers until June 30, 2005. Since Admin held this significant responsibility until the establishment of the Office of Enterprise Technology and was not invited to discuss the report findings and recommendations at the November 23, 2005 exit conference, I appreciate the opportunity to comment about the report, especially Admin's efforts to resolve prior audit issues. I want to affirm at the outset that I concur entirely with the need for increased attention to, and discipline around, information technology security. In today's environment, we can afford nothing less. And, in the year or so that I have been in this position, I have demonstrated this attention both through the Governor's assignment to me of a response to website security issues last spring, and the focus on enterprise security through the Drive to Excellence.

Turning to the report, however, the last page indicates that prior audit issues were not adequately addressed. In my view, this statement might mislead readers to believe that Admin's InterTechnologies Group (ITG) disregarded your office's prior audit recommendations and took no further corrective action than what was reported in the 2002 report.

Admin has consistently recognized that the audit issues raised in the 2000 and 2002 reports represented serious security weaknesses. ITG personnel persevered to strengthen the security control weaknesses limited only by available resources and worked diligently to implement the recommendations you suggested. We also engaged your IT audit professionals in discussions from time to time about whether ITG's progress-to-date and planned corrective actions were acceptable at minimizing security risks, just to ensure that we were addressing your staff's concerns in an appropriate manner. I believe that ITG personnel made considerable security control improvements that deserve further mention.

To demonstrate Admin's commitment to resolve the audit issues, the following examples of corrective actions taken during the past three fiscal years are offered:

- By July 2002, ITG personnel developed and implemented a new re-certification process that enabled staff to review each account with certain powerful ACF2 privileges, to assess the necessity and appropriateness of each security privilege, and to re-certify or remove this privilege as warranted. By December 2004, ITG staff completed written procedures for the re-certification process. (These actions address prior audit recommendation #4.)
- By April 2003, ITG personnel subgrouped Production Support and Computer Operations major access groups into various categories and subsequently limited functional access to data and resources by each category. (This action addresses prior audit recommendation #1.)
- By April 2003, ITG personnel completed an assessment of accounts with certain powerful security privileges and limited access only to those who needed it to perform certain automated or administrative processes. For example, ITG reduced the number of logonids with the NON-CNCL privilege from 26 to 19; ITG found that the 19 are necessary and appropriate for mainframe start-up or business recovery purposes. (This action addresses prior audit recommendation #2.)
- In the fall of 2002, ITG installed an ACF2 upgrade but did not remove the Violation Exit as the OLA initially recommended. ITG staff met with OLA IT professionals about this action; the auditors expressed concern about TSO (Time Sharing Option) users who used the exit. To address this concern, ITG staff created rules for the TSO logonids and developed automated procedures for performing a daily check to see if newly added TSO logonids have rules written first to prevent their unauthorized read-only access to data. (This action addresses prior audit recommendation #5.)
- By December 2003, ITG personnel had added compensating controls the ACF2 developers designed for all but one account – a started task with the RESTRICT privilege. For this account, ITG staff added mitigating controls by making a program change that eliminated a job function from the logonid. Again, ITG relies on the re-certification process to identify those accounts without passwords that require compensating controls. (These actions address prior audit recommendation #3.)
- By January 31, 2004, ITG completed documentation describing ACF2 access authorizations for 1,634 data set rules and nearly all (99.8%) of the 6601 resource rules. A primary obstacle in completing this task was researching and identifying the owners of the rules since many were very old. In this process, ITG also developed criteria for inclusion in the USERDATA field in ACF2 rules. Newly created or recently modified rules are subject to review during the periodic rule monitoring process. (This action addresses prior audit recommendation #6.)
- ITG, in its security leadership role, also informed agency ACF2 administrators that they needed to review and document their 300 data access rules and 1300 resource rules. About 80% of these rules were documented. Also, ITG encouraged the OLA

auditors to address the agency administrators' documentation requirement in the respective agency audit reports. (This action addresses prior audit recommendation #6.)

Admin believed that it had addressed all of the ACF2 prior audit issues to the best of its ability and with available resources. ITG staff always recognized that, as new products emerge and personnel changes occur, new risks also emerge that could pose a threat to mainframe data. Thus, to protect the integrity of the data that resides on the state's mainframe computers against unauthorized use or loss, ITG staff were charged with continuously strengthening mainframe security controls to address new risks.

Thank you for the opportunity to respond to the report findings.

Best regards,

/s/ Dana Badgerow

Dana Badgerow
Commissioner

cc: Gopal Khanna, Office of Enterprise Technology