OLA

OFFICE OF THE LEGISLATIVE AUDITOR
STATE OF MINNESOTA

Financial-Related Audit

Department of Human Services
MAXIS Data Integrity Audit

AUGUST 15, 2002 **02-53**

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

Linda Anderson, Acting Commissioner
Minnesota Department of Human Services

We have conducted an information technology audit of select componenets of the MAXIS computer system. The primary purpose of this audit was to determine if the Department of Human Services restricted access to MAXIS computer programs and data to only those persons who needed such clearance. We also examined the department's procedures for controlling changes to MAXIS computer programs. Our audit scope included a review of the controls that the department had implemented as of March 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 Human Services 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 the Department of Human Services. This restriction is not intended to limit the distribution of this report, which was released as a public document on August 15, 2002.

/s/ James R. Nobles

James R. Nobles
Legislative Auditor

/s/ Claudia J. Gudvangen

Claudia J. Gudvangen, CPA
Deputy Legislative Auditor

End of Fieldwork: April 10, 2002

Report Signed On: August 12, 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

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, CPA	Auditor
Eric Wion, CPA, CISA	Auditor

Exit Conference

We discussed the results of the audit with the following staff of the Department of Human Services at an exit conference on August 2, 2002:

Dennis Erickson	Assistant Commissioner, Finance & Manangement Operations
Jeanette Taylor Jones	Assistant Commissioner, Economic & Community Support Strategies
Johanna Berg	Chief Information Officer
Chris Zehoski	Director, Information & Technology Strategies
Kate Wulf	Director, MAXIS Division
Rita Sjoberg	Manager, Systems Management & Production Control
David Ehrhardt	Director, Internal Audit

Report Summary

The Department of Human Services developed a complex security infrastructure to protect the integrity and confidentiality of MAXIS data. However, this security infrastructure contained several significant weaknesses:

- Many employees and contractors had extremely powerful security clearances that they did not need to fulfill their job duties. (Finding 2, page 6)

- The department did not deploy appropriate controls over some computer programs that are part of the MAXIS nightly scheduled batch processing environment. Computer programs that are used for scheduled batch processing are risky because they do not require a password and typically have extremely powerful security clearances. Unauthorized changes to these programs could lead to a disastrous loss of data or the unauthorized disclosure of confidential information. (Finding 3, page 7)

Inadequate oversight of the overall MAXIS security infrastructure allowed these security weaknesses to go undetected.

- The department has not performed a complete information technology risk assessment of MAXIS for many years. It is imperative to periodically reassess information technology risks because computer systems and the organizations that manage those systems constantly change. Furthermore, new information technology vulnerabilities surface daily that could adversely impact the adequacy of security controls. (Finding 1, page 5)

Chapter 1. Introduction

This information technology audit assessed the adequacy of data integrity and confidentiality controls in the MAXIS computer system. Data integrity controls help protect the accuracy and completeness of important data. Restricting system access and controlling changes to computer programs are examples of data integrity controls. Confidentiality controls help ensure that sensitive data, such as social security numbers and medical records, cannot be seen by unauthorized individuals.

The Department of Human Services uses MAXIS to determine eligibility, compute benefit amounts, and control payments for a variety of different public assistance programs, including:

- Minnesota Family Investment Plan
- Food Stamps
- General Assistance
- Minnesota Supplemental Aid
- Group Residential Housing
- Medical Assistance
- General Assistance Medical Care

The MAXIS system is one of the largest computer systems in state government. MAXIS processes approximately 94,100 cash, 241,600 food, and 107,200 medical benefit cases each month. Total monthly food and cash assistance provided by the system exceeds $44,000,000. At the time of our audit, over 7,000 county and state employees had access to MAXIS. These employees used the system to process over 1.4 million transactions each day.

Over 110 information technology professionals in the Department of Human Services maintain MAXIS and its complex security infrastructure. However, the department also relies on work done by employees in the Department of Administration's InterTechnologies Group (InterTech). InterTech employees operate the state's central mainframe computing center, which houses the MAXIS software. InterTech also supports the network that provides connectivity to all 87 counties.

Chapter 2 discusses the scope, objectives, and methodology that we used to conduct this information technology audit. Chapter 2 also discusses the conclusions that we reached and offers recommendations to improve the system's security infrastructure.

Chapter 2. MAXIS Data Integrity Controls

Chapter Conclusions

The Department of Human Services developed a complex security infrastructure to protect the integrity and confidentiality of MAXIS data. However, this security infrastructure contained several significant weaknesses. Of greatest concern, the department did not deploy appropriate controls over some computer programs that are part of the nightly scheduled batch processing environment. The department also granted many employees powerful security clearances that they did not need to fulfill their job duties.

Ongoing security infrastructure maintenance could have alerted the department to the nightly batch processing weaknesses and the large number of employees with inappropriate clearances. The department did not perform periodic risk assessments to reaffirm the appropriateness of security controls. It also did not periodically recertify employees' access rights. These ongoing maintenance activities are important because they help ensure the continued effectiveness of security controls.

The Department of Human Services deployed several layers of security tools to protect the integrity and confidentiality of MAXIS data:

- The MAXIS system has embedded security features that define specific screens that people can use to view and update data.

- A software package called Natural restricts access to information stored in the database that is used by the MAXIS system.

- A security software package called ACF2 validates the identity of people who try to access the mainframe computer that houses MAXIS. ACF2 also restricts access to the data and computer programs underlying the system.

Collectively, these security tools help the department enforce an appropriate separation of duties for both end-users of MAXIS and employees who manage the system. For example, the department defined numerous security groups to limit county employees to the specific screens that they need to fulfill their job duties. This helps prevent individual employees from performing all benefit processing activities without independent oversight. The department also defined security groups to control its information technology professionals that maintain MAXIS computer programs and data. These security groups help ensure that information technology professionals do not bypass the department's computer program change control and quality assurance procedures.

Audit Objective and Methodology

This audit assessed the adequacy and effectiveness of controls that protect the integrity and confidentiality of MAXIS data. Specifically, we designed our work to answer the following questions:

- Has the Department of Human Services implemented controls to restrict access to MAXIS screens, software, and data to only those persons who need such clearance to fulfill their normal job duties?

- Has the Department of Human Services implemented controls to ensure that all changes to MAXIS software are properly authorized and thoroughly tested?

To answer these questions, we interviewed and obtained documentation from information technology professionals in the Department of Human Services. We also used computer-assisted audit tools to analyze ACF2, Natural, and MAXIS security data. Finally, we tested a sample of software changes to determine if those changes followed the department's change control methodology.

Our audit scope included reviewing the procedures used to approve and monitor county employee security clearances. However, we did not test the clearances granted to specific county employees. The Office of the State Auditor does that testing during their annual financial audits of Minnesota counties. Our scope also did not assess the adequacy of electronic benefit transfer controls, which are reviewed semiannually by another audit organization.

Evaluation Criteria

We obtained our evaluation criteria from the Control Objectives for Information and Related Technology (COBIT), published by the Information Systems Audit and Control Foundation. The mission of COBIT is:

> *To research, develop, publicize, and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.*

The COBIT Framework includes 34 high-level control objectives and 318 detailed control objectives, grouped in the following four domains:

Planning and Organization

This domain covers strategic planning and concerns the ways that information technology can best contribute to the achievement of business objectives. It addresses the need to plan, communicate, and manage a strategic vision.

Acquisition and Implementation	This domain includes control objectives that pertain to acquiring, developing, and implementing information technology solutions. It also covers control objectives that pertain to changing existing systems.
Delivery and Support	This domain includes the processes that must be in place to deliver information technology services on a daily basis. Some of these processes include ensuring systems security and managing data.
Monitoring	This domain addresses the need to regularly assess the quality of information technology processes. It addresses management's oversight of the control processes and independent assurance provided by internal and external audits.

Conclusions

The Department of Human Services developed a complex security infrastructure to protect the integrity and confidentiality of MAXIS data. However, as discussed in Finding 1, the department has not performed important ongoing maintenance to ensure the continued effectiveness of these controls. As discussed in Finding 2, many of the department's employees and contractors had extremely powerful security clearances that they did not need to fulfill their job duties. Finding 3 discusses significant nightly batch processing security weaknesses that came to our attention. The department could have detected these weaknesses by periodically recertifying employee security clearances and performing ongoing information technology risk assessments.

Audit Findings and Recommendations

1. The department has not performed important activities to validate the continued effectiveness of MAXIS security controls.

Although the department prepares periodic security reports for several federal agencies, which helps it identify key security controls that are currently in place, the department does not conduct formal risk assessments on a regular basis. Formal risk assessments are generally more detailed and have a much broader purpose. Specifically, they attempt to identify vulnerabilities that existing security controls may not address. Security controls for large systems like MAXIS need to be the product of a never ending risk management process. There are many information technology risk assessment tools and methodologies to assist in the process. However, most include steps to identify potential system vulnerabilities, estimate the likelihood of their exploit, and assess the potential impact. The resulting risk assessment data helps organizations design security controls that are commensurate with risk. It is imperative to periodically repeat this risk assessment process because computer systems and the organizations that manage those systems

constantly change. Furthermore, new information technology vulnerabilities surface daily that could adversely impact the adequacy of security controls.

Assigning MAXIS security oversight responsibility to a single employee may help the department better coordinate risk management and security infrastructure maintenance activities. At the time of our audit, many information technology professionals performed MAXIS security duties. However, none of these employees had a global understanding of MAXIS security or overall responsibility for managing the entire infrastructure. In Findings 2 and 3, we discuss several significant security weaknesses that could have been detected by better security infrastructure maintenance procedures. We also brought to the department's attention other less critical security weaknesses – most of which could have been detected by more proactive security management.

Recommendation:

- *The department should designate an employee to coordinate MAXIS risk management and security infrastructure maintenance tasks.*

2. Many employees and contractors had inappropriate security clearances.

Many of the department's employees and contractors had powerful security clearances that they did not need to fulfill their job duties. Some groups of people had broad clearance to read MAXIS data, including confidential beneficiary information. After examining these groups, we identified many individuals whose job responsibilities did not require such clearance. We also found an excessive number of people with clearance to change MAXIS data, including critical computer programs.

Most people with inappropriate clearances were members of powerful security groups that had not been properly defined. Organizations typically define security groups to grant homogeneous groups of people consistent and targeted security clearances. For example, all computer programmers may be assigned to a single security group. When used properly, security groups provide a mechanism to separate classes of employees with incompatible job duties. During our audit, we found extremely powerful MAXIS security groups that were not limited to select groups of employees with similar security needs. For example, 141 information technology professionals and contractors were members of a security group that had the ability to alter a wide array of MAXIS data and computer programs. Few people in this group actually needed such broad clearance.

The department did not have a process to periodically reassess the appropriateness of security clearances. Therefore, excessive security clearances granted to employees and contractors went unchallenged for extended periods. In fact, our audit identified some people who no longer worked for the MAXIS Division who still had powerful security clearances.

Recommendations:

- *The department should ensure that all MAXIS security clearances are commensurate with employees' job duties.*

- *The department should develop a process to periodically recertify the appropriateness of all MAXIS security clearances.*

3. Computer programs used for scheduled batch processing were not properly controlled or secured.

The department did not have procedures to control changes to sensitive computer programs that are used to process data at night. Furthermore, many of the libraries that housed those computer programs were not appropriately secured.

Most major computer systems rely on a large overnight batch stream to perform mission critical data processing. For example, the MAXIS nightly batch stream contains hundreds of jobs that run at specific times or after the successful completion of other jobs. The computer programs that initiate these scheduled jobs are written in a special language called Job Control Language, or JCL. These JCL programs are very risky because they do not require passwords and are often granted extremely powerful security clearances. In fact, unauthorized changes to these JCL programs could lead to the disastrous loss of data or unauthorized disclosure of confidential information.

Our security testing identified many people with inappropriate clearance to change sensitive MAXIS JCL programs. Some of these inappropriate clearances resulted from inadequate communication between the department's security officers and employees who work for the Department of Administration's Intertechnologies Group. Other inappropriate clearances resulted from security groups that the department had not properly defined. When questioned, security officers told us that the department did not have procedures that outlined who should be cleared to change JCL or how those changes should be controlled.

Recommendations:

- *The department should restrict access to MAXIS JCL programs to only those employees who need access to fulfill their job duties.*

- *The department should define change control procedures for JCL computer programs.*

August 8, 2002

James R. Nobles, Legislative Auditor
Office of the Legislative Auditor
Centennial Office Building
658 Cedar Street
St. Paul, MN 55155

Dear Mr. Nobles:

The enclosed material is the Department of Human Services response to the findings and recommendations included in the draft audit report on the data integrity of the department's MAXIS computer system. It is our understanding that our response will be published in the Office of the Legislative Auditor's final audit report.

The Department of Human Services policy is to follow-up on all audit findings to evaluate the progress being made to resolve them. Progress is monitored until full resolution has occurred. If you have any further questions, please contact David Ehrhardt, Internal Audit Director, at (651) 282-9996.

Sincerely,

/s/ Linda Anderson

Linda Anderson
Acting Commissioner

Enclosure

cc: Christopher Buse

Department of Human Services
Responses to the Legislative Audit Report on
MAXIS Data Integrity

Audit Finding #1

The department has not performed important activities to validate the continued effectiveness of MAXIS security controls.

Audit Recommendation #1

The department should designate an employee to coordinate MAXIS risk management and security infrastructure maintenance tasks.

Department Response #1

Several security reviews have been conducted focusing on various parts of the operation. The Federal MAXIS Biennial Security Report addresses the use of the administrative controls and physical barriers necessary to prevent unauthorized entry into sensitive MAXIS/EBT areas. It also reviews the software security and backup/fall back procedures required to ensure the security of the MAXIS system. The Internal Revenue Service's Safeguard Review Report and audits ensure that adequate safeguards are in place to protect the confidentiality of tax returns and tax return information. The Social Security Administration conducts regular audits that verify proper protection of social security information. The Office of the State Auditor's county single audit reports review the data input authorization input control procedures in place at county offices. Other informal studies have also addressed security issues.

We agree with the recommendation that MAXIS should designate a single employee to coordinate security and oversee ongoing security risk assessment. However given the current state budget shortfall and the state's hiring freeze, we will need to look into securing additional resources for a new position.

Person Responsible: Kate Wulf, Director, MAXIS Division

Estimated Completion Date: June 30, 2003

Audit Finding #2

Many employees and contractors had inappropriate security clearances.

Audit Recommendation #2-1

The department should ensure that all MAXIS security clearances are commensurate with employee's duties.

Department of Human Services
Responses to the Legislative Audit Report on
MAXIS Data Integrity

Department Response #2-1

The department agrees with the recommendation. Since the audit's fieldwork was completed, security clearances have been reassessed for users identified in the audit. Clearances have been removed or revised commensurate with the employees' job duties. Security groups have also been reexamined. As a result of this review, some members were either removed entirely from the system or moved to groups that were appropriate to their job responsibilities.

Person Responsible: Kate Wulf, Director, MAXIS Division

Estimated Completion Date: Completed

Audit Recommendation #2-2

The department should develop a process to periodically recertify the appropriateness of all MAXIS clearances.

Department Response #2-2

The department agrees with the recommendation. This recommendation has already been implemented for county users, and will be implemented in near future for all other users.

Person Responsible: Kate Wulf, Director, MAXIS Division

Estimated Completion Date: February 28, 2003

Audit Finding #3

Computer programs used for scheduled batch processing were not properly controlled or secured.

Audit Recommendation #3-1

The department should restrict access to MAXIS JCL programs to only those employees who need access to fulfill their job duties.

Department Response #3-1

The department agrees with the recommendation. MAXIS system security staff met with other DHS security staff about the exposure identified in the audit. JCL has been already been revised to remove some exposure and more changes are planned. Security changes described under finding #2 also addressed this problem.

Department of Human Services
Responses to the Legislative Audit Report on
MAXIS Data Integrity

Person Responsible: Kate Wulf, Director, MAXIS Division

Estimated Completion Date: February 28, 2003

Audit Recommendation #3-2

The department should define change control procedures for JCL computer programs.

Department Response #3-2

The department agrees with the recommendation. MAXIS System Operations and Technical staff are meeting to discuss options.

Person Responsible: Kate Wulf, Director, MAXIS Division

Estimated Completion Date: February 28, 2003