PERFORMANCE AUDIT
OF THE

GENERAL CONTROLS OF THE MEDICAID MANAGEMENT INFORMATION SYSTEM (MMIS)

DEPARTMENT OF INFORMATION TECHNOLOGY AND
DEPARTMENT OF COMMUNITY HEALTH

February 2005

39-596-04

"...The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof."

– Article IV, Section 53 of the Michigan Constitution

Audit report information may be accessed at:
http://audgen.michigan.gov

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit
General Controls of the Medicaid Management Information System (MMIS)
Department of Information Technology (DIT) and Department of Community Health (DCH)

Report Number:
39-596-04

Released:
February 2005

MMIS is the automated management and control system for the Michigan Medical Assistance Program (Medicaid). Medicaid, created under Title XIX of the Social Security Act, provides medical services for indigent persons in the general categories of families with dependent children; the aged, blind, and disabled; and other targeted groups that meet income eligibility standards. The primary functions of MMIS include claims processing, prior authorization of client services, recipient eligibility, provider enrollment, surveillance and utilization review, management and administrative reporting, and reference files.

Audit Objective:
To assess the effectiveness of DIT and DCH's information system security program in assessing risk, developing security policies, assigning responsibilities, and monitoring computer related controls for the MMIS application.

Audit Conclusion:
DIT and DCH's information system security program was ineffective.

Material Condition:
DIT and DCH's information system security program did not provide adequate security for MMIS. Without adequate security, DIT and DCH cannot ensure that MMIS is sufficiently protected from loss, misuse, or unauthorized access to or modification of information. (Finding 1)

Reportable Condition:
DIT had not established clear assignments of responsibility and accountability for all information technology personnel who support MMIS (Finding 2).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DIT and DCH's controls to prevent and detect unauthorized access to operating system, system software, and MMIS application and data files.

Audit Conclusion:
DIT and DCH's controls to prevent and detect unauthorized access to operating system, system software, and MMIS application and data files were ineffective.

Material Conditions:
DIT had not established controls to effectively manage and control access to operating system accounts. As a result, DIT could not establish individual accountability for all system activities. (Finding 3)

DIT had not properly secured access to operating system, system software, and MMIS application and data files. As a result, DIT could not ensure that all access was proper and authorized. (Finding 4)

DIT had not implemented effective system security and password controls over MMIS's mainframe operating system. Improving system security and password controls will help DIT provide reasonable assurance that computer resources are protected against unauthorized modification or disclosure. (Finding 5)

Reportable Condition:
DIT had not established effective procedures to document and manage its MMIS catalog and file structure (Finding 6).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DIT and DCH's controls to prevent and detect unauthorized changes to MMIS production data and application programs.

Audit Conclusion:
DIT and DCH's controls to prevent and detect unauthorized changes to MMIS production data and application programs were somewhat effective.

Material Condition:
DIT had not established complete controls over program and data changes. As a result, DIT could not ensure that only authorized, tested, documented, and approved changes to MMIS programs and data were placed into production. (Finding 7)

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DIT and DCH's backup and disaster recovery procedures to ensure the continued service of MMIS.

Audit Conclusion:
DIT and DCH had established effective backup procedures. However, DIT and DCH had not established effective disaster recovery procedures to ensure the continued service of MMIS.

Material Condition:
DIT and DCH had not fully developed and tested a disaster recovery plan for MMIS. Without a detailed, documented, and tested disaster recovery plan, DIT and DCH cannot ensure continued operation and processing of MMIS in the event of a disaster or other service disruption. (Finding 8)

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:
Our audit report contains 8 findings and 8 corresponding recommendations. DIT and DCH's preliminary responses indicate that they agreed with all of the findings and will comply with all of the recommendations.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: http://audgen.michigan.gov

Michigan Office of the Auditor General
201 N. Washington Square
Lansing, Michigan 48913

Thomas H. McTavish, C.P.A.
Auditor General

Scott M. Strong, C.P.A., C.I.A.
Deputy Auditor General

STATE OF MICHIGAN
OFFICE OF THE AUDITOR GENERAL
201 N. WASHINGTON SQUARE
LANSING, MICHIGAN 48913
(517) 334-8050
FAX (517) 334-8079

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

February 25, 2005

Ms. Teresa M. Takai, Director
Department of Information Technology
Landmark Building
Lansing, Michigan
and
Ms. Janet Olszewski, Director
Department of Community Health
Lewis Cass Building
Lansing, Michigan

Dear Ms. Takai and Ms. Olszewski:

This is our report on the performance audit of the General Controls of the Medicaid Management Information System (MMIS), Department of Information Technology and Department of Community Health.

This report contains our report summary; description of system; audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agencies' responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a formal response within 60 days after release of the audit report.

We appreciate the courtesy and cooperation extended to us during this audit.

AUDITOR GENERAL

This page left intentionally blank.

TABLE OF CONTENTS

GENERAL CONTROLS OF THE MEDICAID MANAGEMENT INFORMATION SYSTEM (MMIS) DEPARTMENT OF INFORMATION TECHNOLOGY AND DEPARTMENT OF COMMUNITY HEALTH

GLOSSARY

Description of System

The Medicaid Management Information System* (MMIS) is the automated management and control system for the Michigan Medical Assistance Program (Medicaid). Medicaid, created under Title XIX of the Social Security Act, provides medical services for indigent persons in the general categories of families with dependent children; the aged, blind, and disabled; and other targeted groups that meet income eligibility standards. The primary functions of MMIS include claims processing, prior authorization of client services, recipient eligibility, provider enrollment, surveillance and utilization review, management and administrative reporting, and reference files.

The Department of Information Technology (DIT) is responsible for providing information technology (IT) services to support MMIS. DIT is responsible for the general controls* impacting MMIS, including IT administration, data center operations, operating system software*, MMIS application* maintenance and development, and physical security.

The Medical Services Administration*, Department of Community Health (DCH), administers the State's Medicaid Program. DCH owns the Medicaid data* and is responsible for MMIS application controls* to ensure that authorized data is processed completely and accurately.

Both DIT and DCH share responsibility for the security of MMIS.

In fiscal year 2002-03, MMIS processed approximately 41 million claims for 1.35 million recipients totaling $4.9 billion dollars. In fiscal year 2002-03, expenditures for the operation and maintenance of MMIS, including modifications for Health Insurance Portability and Accountability Act (HIPAA) privacy requirements, totaled approximately $57.6 million dollars.

* *See glossary at end of report for definition.*

Audit Objectives

Our performance audit* of the General Controls of the Medicaid Management Information System (MMIS), Department of Information Technology (DIT) and Department of Community Health (DCH), had the following objectives:

1. To assess the effectiveness* of DIT and DCH's information system security program in assessing risk, developing security policies, assigning responsibilities, and monitoring computer related controls for the MMIS application.

2. To assess the effectiveness of DIT and DCH's controls to prevent and detect unauthorized access to operating system, system software*, and MMIS application and data files.

3. To assess the effectiveness of DIT and DCH's controls to prevent and detect unauthorized changes to MMIS production data and application programs.

4. To assess the effectiveness of DIT and DCH's backup and disaster recovery procedures to ensure the continued service of MMIS.

Audit Scope

Our audit scope was to examine the information processing and other records of the Department of Information Technology and Department of Community Health relevant to the general controls of the Medicaid Management Information System. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances.

Audit Methodology

Our methodology included examination of DIT and DCH's information processing and other records primarily for the period October 1, 2002 through May 31, 2004. Our audit

* *See glossary at end of report for definition.*

fieldwork was performed from February through June 2004. To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We conducted a preliminary review to identify the information processing functions that support MMIS. We obtained and reviewed DIT and DCH policies and procedures for establishing information system security, administering access to MMIS and its operating system, managing changes to production data and application programs, and ensuring continued service. We used the results of our review to determine the extent of our detailed analysis and testing.

2. Detailed Analysis and Testing Phase

   We performed an assessment of internal control* pertaining to: (a) the effectiveness of DIT and DCH's information system security program; (b) the effectiveness of DIT and DCH's controls to prevent and detect unauthorized access to operating system, system software, and MMIS application and data files; (c) the effectiveness of DIT and DCH's controls to prevent and detect unauthorized changes to MMIS production data and application programs; and (d) the effectiveness of DIT and DCH's backup and disaster recovery procedures to ensure the continued service of MMIS. Specifically, we assessed:

   a. Effectiveness of Information System Security Program:

      (1) We assessed the assignment of responsibility and accountability for the management and security over MMIS. We assessed the independence, authority, and effectiveness of the security officer function.

      (2) We determined if DIT and DCH had established a proper segregation of duties over incompatible job functions.

      (3) We reviewed DIT's security related personnel policies and procedures.

      (4) We reviewed DIT and DCH's process for assessing, monitoring, and reducing information system security risk.

* *See glossary at end of report for definition.*

b. Effectiveness of Controls to Prevent and Detect Unauthorized Access:

(1) We reviewed and assessed DIT and DCH's policies and procedures for granting access to operating system, system software, and MMIS application and data files.

(2) We tested users' access rights to operating system, system software, and MMIS application and data files to ensure that access was granted in accordance with established policies and procedures.

(3) We tested controls over the granting and monitoring of administrative access.

c. Effectiveness of Controls to Prevent and Detect Unauthorized Changes:

(1) We reviewed and assessed the effectiveness of DIT and DCH's policies and procedures for managing changes to MMIS data and application programs.

(2) We selected a sample of MMIS program changes and verified that appropriate authorizations and approvals were obtained.

(3) We tested DIT procedures to ensure that only documented, tested, and authorized changes are moved into production.

d. Effectiveness of Backup and Disaster Recovery Procedures:

(1) We reviewed and assessed DIT and DCH's backup procedures and file retention policies.

(2) We reviewed and assessed DIT and DCH's disaster recovery plan.

3. Evaluation and Reporting Phase

We evaluated and reported on the results of the detailed analysis and testing phase.

Agency Responses

Our audit report contains 8 findings and 8 corresponding recommendations. DIT and DCH's preliminary responses indicate that they agreed with all of the findings and will comply with all of the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agencies' written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and Department of Management and Budget Administrative Guide procedure 1280.02 require DIT and DCH to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF INFORMATION SYSTEM SECURITY PROGRAM

COMMENT

Background: An information system security program documents management's commitment to addressing security risks and establishes the framework for the organization's information system security control structure. An information system security program includes assessing security risks, developing and implementing effective security procedures, and monitoring the effectiveness of the security procedures.

In summer 2002, the State's chief information security officer conducted a Statewide risk assessment to document the status of information security in State agencies. As a result, the Department of Information Technology's (DIT's) Office of Enterprise Security developed an Information Technology Security Framework that included specific recommendations for DIT and State agencies that, if implemented, could improve information system security and reduce security risks.

Audit Objective: To assess the effectiveness of DIT and the Department of Community Health's (DCH's) information system security program in assessing risk, developing security policies, assigning responsibilities, and monitoring computer related controls for the MMIS application.

Conclusion: DIT and DCH's information system security program was ineffective. Our assessment disclosed one material condition*. DIT and DCH's information system security program did not provide adequate security* for the Medicaid Management Information System (MMIS) (Finding 1). Our assessment also identified a reportable condition* related to assignment of responsibility (Finding 2).

FINDING

1. Information System Security Program

   DIT and DCH's information system security program did not provide adequate security for MMIS. Without adequate security, DIT and DCH cannot ensure that

* *See glossary at end of report for definition.*

MMIS is sufficiently protected from loss, misuse, or unauthorized access to or modification of information. Our review disclosed:

a. DIT had not assigned responsibility for mainframe computer* security to an individual knowledgeable in the technology and security of MMIS's mainframe operating system. In addition, DIT and DCH had not assigned responsibility for MMIS application security to an individual knowledgeable in the MMIS application and the controls used to protect it.

   We found that individuals other than the appointed security officer performed security functions.

   The effectiveness of an organization's security program is directly impacted by the way responsibility for overseeing its implementation is assigned. Security officers play a key role in developing, communicating, and monitoring compliance with security policies and reporting these activities to senior management. As such, the security officers should have sufficient experience and training in information technology (IT) and security concepts as well as be provided with the authority and resources needed to monitor compliance with established policies and procedures.

b. DIT and DCH had not established a security plan for MMIS. Without a security plan, DIT and DCH cannot ensure that MMIS security requirements are appropriately addressed.

   The purpose of a security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The security plan also identifies responsibilities and expected behavior of all individuals who access the system. The plan should reflect input from the various managers with responsibilities concerning the system, including information owners, computer operations, technical support, and security.

c. DIT and DCH had not performed an information system security risk assessment for the MMIS application and MMIS's operating system.

* *See glossary at end of report for definition.*

An information system security risk assessment is necessary to ensure that relevant threats and vulnerabilities are identified and to determine the effectiveness of current or proposed controls. For example, the risk assessment should identify areas of vulnerability related to personnel, facilities, hardware, system software, operating systems, and applications. DIT and DCH should assess risks posed by both authorized and unauthorized users trying to access the system.

d. DIT did not monitor for sensitive activities impacting security. In addition, DIT did not monitor for security violations. As a result, DIT did not have the ability to detect inappropriate or unauthorized access to MMIS.

   To establish effective security, DIT should develop procedures for logging and reviewing security-related events, such as unauthorized access attempts, access to sensitive data and resources, access using privileged accounts, and access grants and modifications made by security personnel. In addition, DIT should ensure that all suspected violations are investigated.

   DIT informed us that it had identified sensitive activities to monitor; however, the logging function had been deactivated.

e. DIT had not established or updated policies and procedures for IT security functions to reflect changes in responsibilities and practices that occurred because of the creation of DIT. Outdated or ineffective policies and procedures increase the risk that responsibility for critical security functions will not be assigned to appropriate personnel or will not be properly and consistently carried out.

   Specifically, DIT should update procedures for assigning security responsibilities as well as granting, modifying, or removing access to mainframe resources and MMIS. In addition, DIT should establish end-user security procedures that explain DIT's information security program and document rules of acceptable behavior and confidentiality practices. DCH drafted an end-user security policy. However, DIT had not implemented the policy.

Title 45, Part 95, section 621 of the *Code of Federal Regulations* requires State agencies to determine appropriate information system security requirements based

on recognized industry standards or standards governing security of federal information systems and information processing, to establish a security program, to perform periodic risk analyses, and to perform information system security reviews. In addition, the Health Insurance Portability and Accountability Act (HIPAA) security rules, effective April 21, 2003, require the State to establish specific security controls by April 21, 2005 to ensure the availability and integrity of electronic protected health information as well as protect the information from unauthorized use or disclosure.

DIT informed us that it did not have the resources necessary to comply with the federal security requirements. However, federal regulations consider the costs incurred in complying with system security provisions as regular administrative costs, which can be funded at the regular federal match rate.

RECOMMENDATION

We recommend that DIT and DCH ensure that the information system security program provides adequate security for MMIS.

AGENCY PRELIMINARY RESPONSE

DIT agreed with the finding and will continue to work with DCH to provide security for MMIS to ensure that MMIS is sufficiently protected from loss, misuse, or unauthorized access to or modification of information. DIT informed us that it is currently working on establishing a security administrator position for MMIS. The security administrator's responsibilities will include performing a risk assessment and developing a security plan for MMIS.

The Medical Services Administration within DCH informed us that it has also appointed a security administrator for MMIS who will meet regularly with the DIT security administrator (once appointed). DCH will work with the DIT security administrator to formalize the security program and to address the issues identified in parts a., b., and c. of the finding. The DCH security administrator will also annually review the MMIS security plan to ensure that it complies with State and federal HIPAA security requirements.

FINDING

2. Assignment of Responsibility

DIT had not established clear assignments of responsibility and accountability for all IT personnel who support MMIS. This increases the likelihood that controls designed to segregate incompatible duties will not be enforced and that job functions will not be performed in accordance with management's directives.

Senior management is responsible for ensuring that all employees fully understand their duties and responsibilities and carry out those responsibilities in accordance with their job descriptions. Management is also responsible for ensuring that adequate resources exist to enforce controls over segregation of incompatible duties.

We identified several critical job functions, such as security administration and database management, for which someone other than the employee identified to us as responsible for the function performed the job. For other responsibilities, such as disaster recovery planning, DIT had not assigned responsibility for the job function.

RECOMMENDATION

We recommend that DIT establish clear assignments of responsibility and accountability for all IT personnel who support MMIS.

AGENCY PRELIMINARY RESPONSE

DIT agreed with the finding. Roles and assignments will be clarified for all IT personnel who support MMIS by January 1, 2005.

EFFECTIVENESS OF CONTROLS TO PREVENT AND DETECT UNAUTHORIZED ACCESS

Background: Access controls ensure the confidentiality, integrity, and availability of computer resources and data. Logical access controls* include computer hardware or software designed to prevent or detect unauthorized access to sensitive files.

* *See glossary at end of report for definition.*

Access control software provides a means of specifying who has access to a system and to specific resources as well as what capabilities authorized users are granted. In addition, access control software provides a means of automatically logging and reporting access activity. Logical access controls should be designed to restrict authorized users to the specific systems, programs, and files that they need for their jobs and to prevent others, such as hackers, from accessing the system at all.

Audit Objective: To assess the effectiveness of DIT and DCH's controls to prevent and detect unauthorized access to operating system, system software, and MMIS application and data files.

Conclusion: DIT and DCH's controls to prevent and detect unauthorized access to operating system, system software, and MMIS application and data files were ineffective. Our assessment disclosed three material conditions. DIT had not established controls to effectively manage and control access to operating system accounts (Finding 3). Also, DIT had not properly secured access to operating system, system software, and MMIS application and data files (Finding 4). In addition, DIT had not implemented effective system security and password controls for MMIS's mainframe operating system (Finding 5). Our assessment also disclosed a reportable condition related to disk management (Finding 6).

FINDING

3. Operating System Accounts

DIT had not established controls to effectively manage and control access to operating system accounts. As a result, DIT could not establish individual accountability for all system activities.

Our review disclosed:

a. DIT did not control access to privileged accounts. Privileged accounts have the ability to bypass operating system controls. Therefore, unauthorized use of privileged accounts could compromise the confidentiality, integrity, and availability of MMIS and the operating system. We noted:

(1) DIT did not assign unique accounts to privileged users. DIT technical support staff shared the administrative and other privileged accounts. To maintain accountability, the sharing of accounts should be prohibited.

DIT technical support staff use administrative accounts to perform certain job responsibilities, such as creating user identifications (IDs), resetting passwords, and configuring the operating system. Current operating system limitations prevent DIT from assigning unique user IDs with comparable privileges or using other system features to authenticate a user's identity.

However, DIT informed us that features of the mainframe security software, if implemented, would allow the assignment of unique user IDs.

(2) DIT did not sufficiently restrict access to certain privileged accounts to DIT technical support staff.

Our review disclosed that access to the privileged accounts was granted to contractors. In addition, we identified one privileged account that was no longer used and one privileged account for which access was granted to a contractor no longer employed by DIT.

Access to privileged accounts should be restricted to a very limited number of personnel whose job responsibilities require that they have access. DIT should establish procedures for granting emergency and temporary access to contractors as needed and for terminating the access when it is no longer needed.

(3) DIT did not monitor activities performed with privileged accounts.

Privileged accounts have the ability to circumvent security and controls. Therefore, activities performed with privileged accounts should be identified, logged, and monitored by management.

DIT informed us that it produced a report of batch jobs granted privileged access. However, DIT did not review the report.

b. DIT did not effectively manage mainframe user accounts. Weaknesses in user account management increase the risk that an unauthorized user might

gain access to sensitive files and confidential data. Our review of user accounts disclosed:

(1) DIT could not identify the owner or business purpose for all user accounts. In particular, we identified one account with unlimited access to MMIS data files for which DIT could not identify the owner or business purpose. Because of the lack of an audit trail and monitoring, DIT could not tell us if the account was being used.

(2) DIT did not remove or disable user accounts that no longer needed access to the operating system. We identified 103 (24%) user accounts from a sample of 431 for which DIT informed us that the owner of the account had departed or access to the operating system was no longer necessary. The timely removal or disabling of user accounts would reduce the risk of unauthorized access and changes to sensitive files and data.

RECOMMENDATION

We recommend that DIT establish controls to effectively manage and control access to operating system accounts.

AGENCY PRELIMINARY RESPONSE

DIT agreed with the finding, for the time period covered by this performance audit, and will continue with its efforts to implement new System Security Management (SSM) software that will satisfy the requirement for managing and controlling access to operating system accounts. SSM will be fully implemented by January 31, 2005.

FINDING

4. Information System Access

DIT had not properly secured access to operating system, system software, and MMIS application and data files. As a result, DIT could not ensure that all access was proper and authorized. Specifically:

a. DIT had not restricted access rights and permissions to operating system, system software, and MMIS application and data files. We identified DIT

employees with access rights that exceeded the rights needed for the employees to perform their work. We also identified files with permissions that granted all users the ability to access and modify the files. Excessive access rights and permissions provide opportunities for individuals to circumvent established controls to protect sensitive files and data.

b. DIT had not removed access to information system catalogs* and files for deleted user accounts. Our analysis identified access rights granted to operating system, system software, and MMIS application and data files for which the user account no longer existed. Deleted accounts that are later re-created will have the same access levels. To prevent improper access, DIT should develop procedures to remove file access when a user account is deleted.

Properly securing information system files would help DIT maintain the integrity of the information system and protect the confidentiality of the data residing on it.

RECOMMENDATION

We recommend that DIT properly secure access to operating system, system software, and MMIS application and data files.

AGENCY PRELIMINARY RESPONSE

DIT agreed with the finding, for the time period covered by this performance audit, and will continue with its efforts to implement controls to ensure proper access and auditing of operating system, system software, and MMIS application and data files.

FINDING

5. System Security and Password Controls

DIT had not implemented effective system security and password controls over MMIS's mainframe operating system. Improving system security and password controls will help DIT provide reasonable assurance that computer resources are protected against unauthorized modification or disclosure.

* *See glossary at end of report for definition.*

Our review disclosed:

a. The mainframe operating system was not designed to enforce strong password rules. The operating system did not require a minimum password length or strong rules for password composition and frequency of use. Weaknesses in password rules increase the risk that a password can be easily compromised.

b. The mainframe operating system was not designed to store passwords in an encrypted format. Users with access to privileged accounts and commands have the ability to access and view passwords. Improper disclosure of users' passwords may diminish DIT's ability to establish accountability for inappropriate system activity and file access.

c. DIT had not configured the mainframe operating system to automatically disable user accounts after a specified number of attempts. In addition, DIT did not monitor for unsuccessful log-in attempts. Disabling user accounts and monitoring for unsuccessful log-in attempts may help DIT prevent and detect unauthorized access.

d. DIT had not implemented encryption for network communications with the mainframe computer. Implementing encryption would protect the confidentiality and integrity of user IDs, passwords, and other MMIS confidential data. HIPAA security requirements include the encryption of network communications if DIT determines the implementation of encryption to be a reasonable and appropriate security measure.

RECOMMENDATION

We recommend that DIT implement effective system security and password controls over MMIS's mainframe operating system.

AGENCY PRELIMINARY RESPONSE

DIT agreed with the finding, for the time period covered by this performance audit, and will continue with its efforts to implement stronger security measures by implementing SSM software. In addition, DIT will install Secure Socket Layer encryption for network communications. These tasks will be completed by February 1, 2005.

FINDING

6. Disk Management

DIT had not established effective procedures to document and manage its MMIS catalog and file structure. A well-documented catalog and file structure would help DIT ensure that critical catalogs and files are properly secured and backed up and that operating costs for items such as disk storage are minimized. Specifically:

a. DIT did not have up-to-date documentation describing the catalog and file structure for MMIS and the mainframe operating system. As such, DIT could not easily identify the purpose and contents for several of its catalogs and files.

b. DIT did not segregate all development and production catalogs and files. We identified catalogs that contained both development and production files. Separate catalogs would decrease the likelihood that the wrong file could be modified and moved into production.

RECOMMENDATION

We recommend that DIT establish effective procedures to document and manage its MMIS catalog and file structure.

AGENCY PRELIMINARY RESPONSE

DIT agreed with the finding, for the time period covered by this performance audit, and will create and institute procedures to document and manage the file and catalog structure.

EFFECTIVENESS OF CONTROLS TO PREVENT AND DETECT UNAUTHORIZED CHANGES

Background: Establishing controls over the modification of application software programs and data helps to ensure that only authorized programs and modifications are implemented. This is accomplished by instituting policies, procedures, and techniques to help ensure that all programs and their modifications are properly authorized, tested, documented, and approved and that access to and distribution of programs is carefully controlled.

Audit Objective: To assess the effectiveness of DIT and DCH's controls to prevent and detect unauthorized changes to MMIS production data and application programs.

Conclusion: DIT and DCH's controls to prevent and detect unauthorized changes to MMIS production data and application programs were somewhat effective. Our assessment identified one material condition. DIT had not established complete controls over program and data changes (Finding 7).

FINDING

7. Program and Data Change Controls

DIT had not established complete controls over program and data changes. As a result, DIT could not ensure that only authorized, tested, documented, and approved changes to MMIS programs and data were placed into production.

Our review disclosed:

a. DIT did not effectively restrict programmer and application technical support staff access to MMIS program and data files. Because these individuals have extensive knowledge of MMIS as well as access to MMIS program and data files, unauthorized changes could occur and not be detected. As such, DIT should limit programmer and application technical support staff access to only the development and test programs.

b. DIT did not make program changes in accordance with established practices designed to ensure that all program changes were properly authorized and documented. Our review of 44 program changes disclosed:

(1) DIT did not link user service requests with the related program changes. Users submit a service request form to initiate a change to an MMIS program or to correct data. However, DIT's procedures did not tie the service request number to the subsequent program change.

(2) DIT could not locate service request forms for 21 (48%) of 44 program changes tested. In addition, DIT did not properly complete any of the 23 service request forms that were located. DIT informed us that 11 of the 21 missing service request forms were for aborted programs or

production problems and that it was not DIT's practice to require a service request form for these circumstances.

Requiring a properly completed service request form for all changes would help DIT ensure that all service requests are clearly communicated and properly authorized.

(3) DIT could not locate program modification request forms for 35 (80%) of 44 program changes tested. DIT system analysts prepare program modification request forms to provide programmers with detailed instructions on how to modify programs.

Completing the program modification request form would help DIT ensure that program changes satisfy user requirements.

(4) DIT could not locate program maintenance forms for 22 (50%) of 44 program changes tested. DIT uses the program maintenance form to document authorizations and approvals of program changes throughout the program change process.

DIT informed us that it was not necessary to maintain the form with the program change documentation. As such, DIT should implement alternative procedures to ensure that all required approvals are documented and maintained.

(5) DIT did not document approvals of user management prior to moving program changes into production. To help ensure that programs operate as intended, when appropriate, MMIS user management should participate in acceptance testing or review test results prior to a change being moved into production.

DIT informed us that it obtained verbal approvals from user management prior to moving a change into production. However, to provide evidence that the change was properly tested and approved, DIT should obtain written approval.

c. DIT had not established complete procedures for program changes and data fixes. For example, DIT's procedures did not reflect the current program

change control process and did not specify the approvals and documentation required to support the change. In addition, DIT had not documented procedures for emergency changes or data fixes.

Documented change control procedures would help ensure that employees understand established controls. Also, documented procedures would increase the likelihood that employees will carry out their responsibilities in accordance with management's intent.

Subsequent to our audit fieldwork, DIT drafted additional procedures to address the weaknesses identified in the change control process.

RECOMMENDATION

We recommend that DIT establish complete controls over program and data changes.

AGENCY PRELIMINARY RESPONSE

DIT agreed with the finding, for the time period covered by this performance audit, and informed us that it has created and instituted procedures to address the program change control process within MMIS. In addition, DIT will create and institute procedures to address the program change control process for the general control areas.

EFFECTIVENESS OF BACKUP AND DISASTER RECOVERY PROCEDURES

Background: Information systems are vulnerable to a variety of disruptions. Many vulnerabilities may be eliminated through technical, management, or operational solutions as part of the organization's risk management or security controls; however, typically it is impossible to completely eliminate all risks. Contingency planning is designed to ensure that essential information systems and services can be recovered quickly after an interruption and that critical and sensitive data is protected. An important part of contingency planning is the development of a disaster recovery plan. The disaster recovery plan documents the detailed procedures required to restore a system, often at an alternative site. Disaster recovery procedures should be periodically tested to ensure that they will function as intended in an emergency situation.

Audit Objective: To assess the effectiveness of DIT and DCH's backup and disaster recovery procedures to ensure the continued service of MMIS.

Conclusion: DIT and DCH had established effective backup procedures. However, DIT and DCH had not established effective disaster recovery procedures to ensure the continued service of MMIS. Our assessment identified one material condition. DIT and DCH had not fully developed and tested a disaster recovery plan for MMIS (Finding 8).

FINDING

8. Disaster Recovery Plan

DIT and DCH had not fully developed and tested a disaster recovery plan for MMIS. Without a detailed, documented, and tested disaster recovery plan, DIT and DCH cannot ensure continued operation and processing of MMIS in the event of a disaster or other service disruption.

Although DIT had a disaster recovery plan for restoring the mainframe operating system, DIT did not have a complete plan for restoring the MMIS application. The disaster recovery plan should contain current and detailed descriptions of all strategies, standards, procedures, schedules, and resources required to complete the disaster recovery process.

DIT and DCH could improve the current disaster recovery plan for MMIS by including information such as:

a. System description and architecture.

b. Identification of all critical IT resources.

c. A definition of an emergency situation.

d. Recovery priorities.

e. Contact information and notification procedures for key personnel, vendors and service partners.

f. Roles and responsibilities of recovery personnel.

g. Identification of all relevant operating and processing procedures.

h. Security requirements.

In addition, DIT and DCH had not conducted recovery tests to confirm their ability to resume operations. Disaster recovery plans for critical systems, such as MMIS, should be tested at least once every two years, whenever significant changes have been made to the plan, or whenever turnover of key people has occurred.

RECOMMENDATION

We recommend that DIT and DCH fully develop and test a disaster recovery plan for MMIS.

AGENCY PRELIMINARY RESPONSE

DIT agreed with the finding, for the time period covered by this performance audit, and will continue with its efforts to fully develop and test the disaster recovery plan for MMIS. DIT informed us that it is currently working on establishing a security administrator position for MMIS. One of the security administrator's responsibilities will be to develop a disaster recovery plan.

DCH informed us that it is prepared to work with DIT in the development and testing of a disaster recovery plan for the current MMIS. In addition, DCH informed us that it is currently bidding for a new MMIS. This bid specifies that the contractor must provide and implement a disaster recovery plan. DCH and DIT will be testing this requirement during the contract implementation period. The new MMIS should be operational by January 2007 with a fully functioning disaster recovery process.

DCH will coordinate its effort with DIT to provide ongoing testing of the disaster recovery plan at least once every two years.

GLOSSARY

adequate security	Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes ensuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls. (Definition taken from Appendix III, "Security of Federal Automated Information Resources," to U.S. Office of Management and Budget Circular A-130, revised.)
application	A computer program designed to help people perform a certain type of work, including specific functions, such as payroll, inventory control, accounting, and mission support.
application controls	Controls directly related to individual applications that help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.
catalog	An area of computer storage used to organize other catalogs and files in a hierarchical structure.
data	Facts and information that can be communicated and manipulated.
DCH	Department of Community Health.
DIT	Department of Information Technology.
effectiveness	Program success in achieving mission and goals.
general controls	The structure, policies, and procedures that apply to an entity's overall computer operations. General controls include an entity-wide security program, access controls,

	application development and change controls, segregation of duties, system software controls, and service continuity controls.
HIPAA	Health Insurance Portability and Accountability Act.
ID	identification.
internal control	The organization, policies, and procedures adopted by agency management and other personnel to provide reasonable assurance that operations, including the use of agency resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition.
IT	information technology.
logical access controls	The use of computer hardware and software to prevent or detect unauthorized access. For example, users may be required to input user ID numbers, passwords, or other identifiers that are linked to predetermined access privileges.
mainframe computer	A multiuser computer designed to meet the computing needs of a large organization. Mainframe computers are used for processing large amounts of data and transactions.
material condition	A reportable condition that could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.
Medicaid	Michigan Medical Assistance Program.

Medicaid Management Information System (MMIS)	The system that processes Medicaid claims submitted to the State as allowed by current State and federal regulations. MMIS supports the Medical Services Administration by processing Medicaid claims and providing information to follow up unpaid claims with medical service providers or recipients.
Medical Services Administration	A DCH entity composed of the Bureau of Medicaid Program Operations and Quality Assurance, the Bureau of Medicaid Financial Management and Administrative Services, and the Bureau of Medicaid Policy and Actuarial Services.
operating system software	The software that controls the execution of other computer programs, schedules tasks, allocates storage, handles the interface to peripheral hardware, and presents a default interface to the user when no application program is running.
performance audit	An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action.
reportable condition	A matter that, in the auditor's judgment, represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner.
SSM	System Security Management.
system software	The set of computer programs and related routines designed to operate and control the processing activities of computer equipment. System software includes the operating system and utility programs and is distinguished from application software.