MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF

GENERAL CONTROLS OF THE OFFENDER MANAGEMENT NETWORK INFORMATION SYSTEM

DEPARTMENT OF CORRECTIONS AND
DEPARTMENT OF INFORMATION TECHNOLOGY

December 2007

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

471-0592-07

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 can be accessed at:
http://audgen.michigan.gov

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit

General Controls of the Offender Management Network Information System

Department of Corrections and Department of Information Technology

Report Number:
471-0592-07

Released:
December 2007

The Offender Management Network Information System (OMNI) is an information processing system that the Department of Corrections (DOC) uses to store and manage offender and employee data. The Department of Information Technology (DIT) provides information technology support services to DOC for OMNI. The services include system development and maintenance, database and operating system security and administration, and backup and recovery management.

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

Audit Conclusion:
DOC and DIT's controls to prevent and detect unauthorized access to OMNI application, data, and operating system files were not effective. We noted one material condition (Finding 1) and two reportable conditions (Findings 2 and 3).

Material Condition:
DOC had not established a comprehensive information systems security program and effective access controls over OMNI (Finding 1).

Reportable Conditions:
DIT and DOC had not fully established security controls over the OMNI databases and operating system (Finding 2).

DOC did not fully develop and monitor audit trails for OMNI data (Finding 3).

Audit Objective:
To assess the effectiveness of DIT's change controls over OMNI program files, database software, and operating system software.

Audit Conclusion:
DIT's change controls over OMNI program files, database software, and operating system software were not effective. We noted one material condition (Finding 4).

Material Condition:
DIT and DOC had not developed a comprehensive change control process for OMNI (Finding 4).

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

Audit Conclusion:
DIT's backup and recovery procedures to ensure the continued service of OMNI were moderately effective. We noted one reportable condition (Finding 5).

Reportable Condition:
DIT had not completely established an effective backup and recovery process for OMNI. In addition, DIT had not developed a comprehensive disaster recovery plan. (Finding 5)

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:
Our audit report contains 5 findings and 6 corresponding recommendations. DOC's and DIT's preliminary responses indicate that they agree with all of the recommendations and will comply with them.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

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

December 28, 2007

Ms. Patricia L. Caruso, Director
Department of Corrections
Grandview Plaza Building
Lansing, Michigan
and
Ms. Teresa M. Takai, Director
Department of Information Technology
George W. Romney Building
Lansing, Michigan

Dear Ms. Caruso and Ms. Takai:

This is our report on the performance audit of General Controls of the Offender Management Network Information System, Department of Corrections and Department of Information Technology.

This report contains our report summary; description of system; audit objectives, scope, and methodology and agency responses and prior audit follow-up; 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 agencies 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 OFFENDER MANAGEMENT NETWORK INFORMATION SYSTEM DEPARTMENT OF CORRECTIONS AND DEPARTMENT OF INFORMATION TECHNOLOGY

Page

INTRODUCTION

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

GLOSSARY

Description of System

The Offender Management Network Information System (OMNI) is an information processing system that the Department of Corrections (DOC) uses to store and manage offender* and employee data. As of June 2007, OMNI contained data for 50,775 prisoners, 16,694 parolees, and 23,111 probationers. OMNI also contains data for 6,513 offenders who have not yet been sentenced.

DOC uses OMNI to process the intake of prisoners into the correctional system and to manage the supervision of parolees and probationers. During the intake of prisoners, DOC enters prisoner and sentencing information into OMNI. The sentencing information is transferred electronically to the Corrections Management Information System (CMIS). CMIS performs the computation of prisoner release dates. For parolees and probationers, DOC uses OMNI to track and record the parole violation process, Parole Board* consideration process, and community supervision. OMNI also contains DOC employee information, including employee identification and photographs, social security numbers, employee caseloads and work locations, and concealed weapon certifications.

In addition, OMNI data is used by the DOC Offender Tracking Information System (OTIS) and the Michigan Department of State Police's Law Enforcement Information Network (LEIN). OTIS provides information to the public about offenders currently or previously in a Michigan prison or on parole or probation under the supervision of DOC. LEIN provides information to criminal justice agencies about individuals, including warrants*, stolen property, and criminal history information.

There are approximately 9,800 OMNI users, including DOC employees, Michigan State police officers, Oakland and Wayne County clerks and police officers, prisoner escape recovery units, Michigan Prisoner ReEntry Initiative community coordinators, prison psychologists, substance abuse test contractors, and other State of Michigan employees. There are approximately 155 user profiles that DOC assigns to users that determine what OMNI modules and data a user can access. Some of the OMNI modules include offender intake, reception center in-processing, offender tracking, offender callout*, probation case administration, and Parole Board administration.

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

The Department of Information Technology (DIT) provides information technology* support services to DOC for OMNI. The services include system development and maintenance, database and operating system security and administration, and backup and recovery management.

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

Audit Objectives

Our performance audit* of General Controls* of the Offender Management Network Information System (OMNI), Department of Corrections (DOC) and Department of Information Technology (DIT), had the following objectives:

1. To assess the effectiveness* of DOC and DIT's controls to prevent and detect unauthorized access to OMNI application, data, and operating system* files.

2. To assess the effectiveness of DIT's change controls* over OMNI program files, database software, and operating system software.

3. To assess the effectiveness of DIT's backup and recovery procedures to ensure the continued service of OMNI.

Audit Scope

Our audit scope was to examine the information processing and other records of the Offender Management Network 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. Our audit procedures, conducted from February through July 2007, generally covered the period May 2002 through July 2007.

Audit Methodology

To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We conducted a preliminary review of OMNI general controls to formulate a basis for defining the audit scope and objectives. Our review included interviewing DOC

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

and DIT personnel, reviewing applicable policies and procedures, and obtaining an understanding of DOC and DIT's information processing functions related to OMNI. We used the results of our preliminary review to determine the extent of our detailed analysis and testing.

2. Detailed Analysis and Testing Phase

We assessed the effectiveness of DOC and DIT's controls to prevent unauthorized access to OMNI application, data, and operating system files. We also assessed the effectiveness of DIT's change controls and backup and recovery procedures:

a. Effectiveness of Access Controls*:

(1) We reviewed DOC's access policies and procedures over the assignment of OMNI user profiles*.

(2) We examined and tested DOC and DIT's access controls over OMNI.

(3) We reviewed and assessed DOC's controls over access to OMNI audit trails.

(4) We reviewed and tested DIT's controls over stored database procedures and triggers that were designed to automatically execute in the database.

(5) We examined and tested DOC and DIT's controls over database and operating system configurations for OMNI.

(6) We tested DOC and DIT's controls over database and operating system user access for OMNI.

b. Effectiveness of Change Controls:

(1) We reviewed DIT's policies and procedures for managing program, database, and operating system changes.

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

(2) We examined and tested the effectiveness of DIT's controls to ensure that only tested and authorized changes are placed into production for OMNI.

c. Effectiveness of Backup and Recovery Procedures:

(1) We interviewed DIT staff to obtain an understanding of backup and recovery controls over OMNI.

(2) We reviewed and evaluated program, database, and server backup and recovery procedures for OMNI.

We use a risk and opportunity based approach when selecting activities or programs to be audited. Accordingly, our audit efforts are focused on activities or programs having the greatest probability for needing improvement as identified through a preliminary review. By design, our limited audit resources are used to identify where and how improvements can be made. Consequently, our performance audit reports are prepared on an exception basis.

Agency Responses and Prior Audit Follow-Up

Our audit report contains 5 findings and 6 corresponding recommendations. DOC's and DIT's preliminary responses indicate that they agree with all of the recommendations and will comply with them.

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 the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require DOC and DIT to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

Within the scope of this audit, we followed up 1 of the 5 recommendations from our October 2005 performance audit of the Accuracy of Prisoner Release Dates, Department of Corrections and Department of Information Technology (47-591-04). We repeated the recommendation in this report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF ACCESS CONTROLS

COMMENT

Audit Objective: To assess the effectiveness of the Department of Corrections (DOC) and the Department of Information Technology's (DIT's) controls to prevent and detect unauthorized access to Offender Management Network Information System (OMNI) application, data, and operating system files.

Conclusion: DOC and DIT's controls to prevent and detect unauthorized access to OMNI application, data, and operating system files were not effective. Our assessment disclosed one material condition*. DOC had not established a comprehensive information systems security program and effective access controls over OMNI (Finding 1). Our assessment also disclosed two reportable conditions* related to OMNI database and operating system security and OMNI audit trails (Findings 2 and 3).

FINDING

1. OMNI Access

DOC had not established a comprehensive information systems security program and effective access controls over OMNI. As a result, DOC cannot ensure the security and integrity* of OMNI data.

In Special Publication 800-53, the National Institute of Standards and Technology* (NIST) recommends that security controls should be employed as a part of a well-defined information systems security program. The security program should be developed based on the results of comprehensive and periodic risk assessments* of data security needs. A comprehensive security program would also define and implement effective policies and procedures for granting access to data and data systems. Our review of OMNI access controls disclosed the following weaknesses:

a. DOC had not established an information security officer position. DOC policy directive 01.04.105, Use of Department Computer Equipment, Software and Services, states that DOC shall appoint a computer security officer. A security officer should have the authority and responsibility to implement an information

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

security program with security policies, standards, and operating procedures for safeguarding OMNI data, including policies regarding granting and monitoring access to OMNI.

b. DOC did not restrict DIT application development staff from administrative access to OMNI. DOC granted 11 application development staff privileged access* to view and modify OMNI data. Application development staff have a detailed knowledge of the OMNI application and application controls. Granting these individuals privileged access to OMNI gives them the ability to bypass established system controls and make changes to OMNI data. Administrative access to OMNI should be granted to only appropriate staff within DOC's Automated Data Systems Section (ADSS).

c. DOC did not have documented policies and procedures for assigning and authorizing access to data. As a result, DOC could not ensure that all user access was appropriate. DOC relied on staff at correctional facilities to authorize access for users. However, we noted:

   (1) DOC did not have a process to ensure that correctional facility staff requesting and approving access had the authority to do so.

   (2) DOC did not provide written policies to correctional facility staff to provide guidance on assigning the appropriate access for a user's job function.

d. DOC did not have an effective process to remove user access. We noted:

   (1) DOC did not remove inactive user accounts. We noted that 3,130 (32%) of 9,764 user accounts had not accessed OMNI in the past 90 days. Of the 3,130 user accounts, we identified 47 (2%) high-risk users with access to critical data.

   (2) DOC did not remove access for all terminated State employees. We noted that 110 (1%) of 9,553 user accounts were assigned to former State employees. Of the 110 user accounts, we identified 6 (5%) high-risk user accounts with access to critical data.

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

Removing unnecessary user accounts may help protect data from unauthorized modification or use.

e. DOC did not ensure appropriate assignment of OMNI user profiles and accounts. We noted:

   (1) DOC did not document the user profiles that are appropriate for each job responsibility. Documenting all user profiles and how they should be assigned based on job responsibilities would help ensure that a single user does not have access rights that would allow the override of critical controls.

   (2) DOC did not maintain documentation that user access had been reviewed and approved for a valid business need for 210 contractors and 359 non-DOC State employees with access to OMNI data.

   (3) DOC did not identify users who were inappropriately assigned multiple user accounts. DOC assigned 294 users more than one user account. Of the 294 users, DOC confirmed that 33 (11%) users were inappropriately assigned multiple user accounts.

f. DOC did not have secure OMNI administrator accounts. Administrator accounts allow access to all data and user accounts in OMNI. We noted 22 administrators with the ability to reset passwords and log in to administrator accounts other than their own. As a result, DOC cannot ensure accountability for administrator actions.

g. DOC did not retain logs of security background checks and security agreements for contractors and other non-DOC State employees at ADSS where access was granted. Therefore, DOC could not document that required security measures were completed for all users who were granted access.

We reported that DOC had not established a comprehensive information systems security program in our performance audit of the Accuracy of Prisoner Release Dates, Department of Corrections and Department of Information Technology, released in October 2005. DOC agreed with our recommendation and informed us that it had formed ADSS and would comply with our recommendation. However, we found that ADSS had not established a comprehensive information security program and effective access controls over OMNI.

RECOMMENDATION

WE AGAIN RECOMMEND THAT DOC ESTABLISH A COMPREHENSIVE INFORMATION SYSTEMS SECURITY PROGRAM AND EFFECTIVE ACCESS CONTROLS OVER OMNI.

AGENCY PRELIMINARY RESPONSE

DOC agrees and informed us that it will comply with the recommendation.

Regarding item a., DOC informed us that, in 2006, it began taking steps to establish an information security officer position within ADSS that would establish security policies, standards, and operating procedures to safeguard OMNI data. DOC also informed us that, due to severe budgetary constraints, the information security officer position was not approved; however, the position was recently approved and is being established.

Regarding item b., DOC informed us that it will develop an appropriate profile for DIT application development staff.

Regarding item c., DOC informed us that it will require correctional facilities to identify authorized requestors who have the authority to request new user access or modifications to a user's access. DOC also informed us that, as part of the duties of the information security officer, it will implement policies to assist DOC staff in determining the appropriate access particular to a user's job function.

Regarding item d., DOC informed us that it will implement policies and procedures to suspend access for inactive OMNI user accounts and remove access for terminated employees. DOC also informed us that it will work with DIT to develop a routine process to identify OMNI accounts not accessed during a specified time frame and will request the access be automatically suspended pending further review. In addition, DOC informed us that it will work with the Bureau of Human Resources to develop procedures to identify employees who have separated from DOC and to remove access to OMNI in a timely manner.

Regarding item e., DOC informed us that it will take steps to improve assignment of appropriate OMNI user profiles based on an employee's job responsibilities and audit all non-DOC users to confirm that documentation is available at ADSS to validate user access for business needs. DOC also informed us that it has started a process to suspend access to a user's existing account when a request for a new account at a different work location is received.

Regarding item f., DOC informed us that it has reduced the number of security administrators to 10 and will work to further limit the number of ADSS security administrators with the development of a security unit. DOC also informed us that it will explore the establishment of audit trails for users with administrator access.

Regarding item g., DOC informed us that it began corrective measures in 2007 by retaining logs of security background checks and security agreements for non-DOC OMNI users. DOC also informed us that it will conduct an audit to confirm that security verification documentation is available at ADSS for all non-DOC OMNI users.

FINDING

2. OMNI Database and Operating System Security

DIT and DOC had not fully established security controls over the OMNI databases and operating system. Fully establishing database and operating system security controls would help ensure that OMNI data is protected from unauthorized modification, loss, or disclosure.

A well-secured database and operating system provide a protected environment to maintain the integrity and confidentiality of data. DIT procedure 1350.11, Security Operational Guidelines for Servers, requires the secure establishment, maintenance, and administration of servers, including operating system software, and the data residing on the servers. Our review of seven OMNI databases and the OMNI operating system disclosed:

a. DIT did not ensure that the databases and operating system were properly secured. We noted:

   (1) DIT did not ensure that all system administrator* accounts had passwords. As a result, DIT could not ensure that the administrator accounts were protected from unauthorized access. An administrator account without a password could allow unauthorized access for anyone knowing the account name. After we brought this to the system administrator's attention, the administrator assigned passwords to all administrator accounts.

   (2) DIT did not remove unnecessary accounts on the operating system. We noted one administrator account that belonged to a terminated employee. The existence of unnecessary accounts could compromise the overall security of OMNI.

   (3) DIT had not established an effective process to ensure that contractors with access to OMNI backup files met security requirements. We noted:

      (a) DIT did not complete national Automated Fingerprint Identification System (AFIS) criminal background checks for 12 (75%) of 16 contractors with access to OMNI backup files. Instead, DIT conducted criminal background checks using the Michigan Department of State Police's Criminal History Records System (CHRS). Although DIT policy does not require that all contractors undergo AFIS background checks, conducting background checks using CHRS will not identify crimes committed outside of Michigan.

      (b) DIT did not have signed security agreements for 3 (19%) of 16 contracts with access to OMNI backup files. Control Objectives for Information and Related Technology* (COBIT) states that contractors

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

who are granted access to information systems should complete security agreements and agree to comply with organizational policies and procedures.

(4) DIT did not encrypt confidential social security numbers and offender information within the databases. Encrypting this confidential data would provide additional security over the data.

(5) DIT did not configure the operating system console to automatically log off after a specified period of inactivity. Automatic log-off reduces the risk of unauthorized access to the operating system account.

(6) DIT had not developed processes to periodically review and secure database and operating system configurations. Periodic review of database and operating system configurations would help ensure that unnecessary accounts and settings are identified and removed.

b. DIT had not established effective security administration and monitoring over the database and operating system files. As a result, DIT could not detect inappropriate and unauthorized activities of database and system administrators. Periodically monitoring system audit logs would help detect DIT misuse of privileged access by the administrators.

c. DIT did not restrict or monitor one DIT executive manager's privileged access to the databases and operating system. As a result, the executive manager had the ability to override database and operating system security controls. The DIT executive manager is responsible for directing and monitoring information technology (IT) staff and managing IT projects. These responsibilities do not require privileged access to the databases and operating system.

d. DIT and DOC had not developed a complete data dictionary for the OMNI databases. As a result, DIT and DOC could not ensure that they maintained data integrity and minimized data redundancy. A data dictionary should contain detailed information about data, including a definition of each data element*. DIT informed us that it had developed a data dictionary but had not created complete data definitions.

RECOMMENDATION

We recommend that DIT and DOC fully establish security controls over the OMNI databases and operating system.

AGENCY PRELIMINARY RESPONSE

DIT and DOC agree, and DIT informed us that it will fully establish security controls over the OMNI databases and operating system by September 30, 2008. DIT informed us that it has removed unnecessary accounts and access to the databases and operating system. DIT also informed us that it has drafted policies and procedures for obtaining background checks, fingerprints, and signed security agreements for all contractors and employees. In addition, DIT informed us that it has established processes to monitor and track configuration files. Further, DIT and DOC informed us that they will work together to ensure that a complete data dictionary is developed for the OMNI databases.

FINDING

3. OMNI Audit Trails

DOC did not fully develop and monitor audit trails for OMNI data. As a result, DOC cannot ensure that it detects the misuse of critical data, such as social security numbers and offender information.

NIST Audit Trail Security Bulletin 97-03 states that audit trails recording user activities, exceptions, and information security events should be maintained to assist in the detection of security violations. DOC and DIT maintained audit trails of all additions, changes, and deletions of data in OMNI and used the logs to restore data and investigate suspected data security violations. However, we noted:

a. DOC did not maintain audit trails of transactions that allowed users to view confidential data. DOC should have an audit trail to investigate inappropriate browsing of social security numbers.

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

b. DOC management did not have the ability to use audit trail data to query and create reports to detect security violations. To investigate a security violation, DOC must request assistance from DIT. The ability to query and create reports would enable DOC to be more proactive in its investigations.

RECOMMENDATION

We recommend that DOC fully develop and monitor audit trails for OMNI data.

AGENCY PRELIMINARY RESPONSE

DOC agrees and informed us that it will comply with the recommendation by coordinating with DIT to incorporate automatic audit trails within tabs that contain confidential data, such as social security numbers, and by integrating audit trails that will generate reports that are accessible by DOC independent of DIT. Furthermore, DOC informed us that it will explore expanding security within OMNI to allow DOC the ability to either block a user from viewing an offender's record or allow only certain user access to view an offender's record.

EFFECTIVENESS OF CHANGE CONTROLS

Audit Objective: To assess the effectiveness of DIT's change controls over OMNI program files, database software, and operating system software.

Conclusion: DIT's change controls over OMNI program files, database software, and operating system software were not effective. Our assessment disclosed one material condition. DIT and DOC had not developed a comprehensive change control process for OMNI (Finding 4).

FINDING

4. Change Control Process

DIT and DOC had not developed a comprehensive change control process for OMNI. As a result, DIT and DOC could not ensure that OMNI program files, database software, and operating system software were protected from corruption and unauthorized changes.

Effective change controls 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 program modifications are properly authorized, tested, and approved and that proper segregation of duties* exists over the change control process.

We reviewed program, database, and operating system change procedures for OMNI. We also tested 38 program and database changes to OMNI from May 2002 to January 2007. DIT has taken steps to develop a change control process; however, our review disclosed:

a. DOC had not fully established effective controls over program and database changes. We noted that 35 (92%) of 38 change request forms did not document the name of the user who requested the change and did not contain management approval. Also, 38 (100%) of 38 changes did not have formal management approval of test results for changes prior to being moved to production.

b. DIT did not fully ensure a proper segregation of duties for the change control process. As a result, unauthorized changes to programs and data could go undetected. We noted that two DIT staff initiated and authorized 2 (5%) of 38 program and database changes. Also, three DIT database administrators and one developer could individually make, test, and implement changes to OMNI programs and data without documented user approvals. Separating the initiating, authorizing, testing, and implementing responsibilities of the program and data change process reduces the risk of an unauthorized change.

c. DIT did not maintain an effective audit trail of all program and database changes. As a result, DIT cannot ensure that only authorized program and database changes were made.

d. DIT did not have a documented process for making emergency program and database changes. As a result, controls for testing and approving emergency changes could be bypassed. Defining the conditions under which emergency changes are allowed as well as testing and approval requirements would help ensure efficient and secure movement of emergency changes to production.

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

RECOMMENDATION

We recommend that DIT and DOC develop a comprehensive change control process for OMNI.

AGENCY PRELIMINARY RESPONSE

DIT and DOC agree, and DIT informed us that it will work together with DOC to develop a comprehensive change control process for OMNI by June 30, 2008. Also, DOC informed us that it will modify its change request forms to include the name of the person who requested the change, the name of the person within ADSS who is requesting the change to be implemented, and the name of the ADSS manager who approved the request. In addition, DOC informed us that, upon staff providing test acceptance in the test application environment, an ADSS manager will document his/her authorization to implement and notify DIT that the change is authorized for implementation.

EFFECTIVENESS OF BACKUP AND RECOVERY PROCEDURES

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

Conclusion: DIT's backup and recovery procedures to ensure the continued service of OMNI were moderately effective. Our assessment disclosed one reportable condition related to backup and recovery (Finding 5).

FINDING

5. Backup and Recovery

DIT had not completely established an effective backup and recovery process for OMNI. In addition, DIT had not developed a comprehensive disaster recovery plan. As a result, DIT cannot fully ensure the integrity and availability* of OMNI in the event of a business disruption.

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

We noted:

a. DIT did not restore data files from tape based only on authorized requests. DIT restored backup files for any persons knowing the necessary backup information. Implementing controls over the restoring of data files would safeguard against inadvertent or malicious data tampering.

b. DIT did not routinely test backup tapes. As a result, backup tapes may not be usable in an emergency. COBIT requires periodically testing backup tapes to ensure that data can be recovered when needed.

c. DIT had not developed and tested a comprehensive disaster recovery plan for OMNI. The lack of a comprehensive plan increases the likelihood that a service interruption will impact OMNI. DIT established Statewide goals for a disaster recovery plan. However, DIT's plan did not include responsibilities of key individuals, resources required to recover OMNI, and provisions for backing up equipment. COBIT states that disaster recovery tests should be scheduled and conducted on a regular basis or upon major changes to the IT infrastructure.

RECOMMENDATIONS

We recommend that DIT completely establish an effective backup and recovery process for OMNI.

We also recommend that DIT develop a comprehensive disaster recovery plan.

AGENCY PRELIMINARY RESPONSE

DIT agrees and informed us that it will establish an effective backup and recovery process for OMNI by December 31, 2008. DIT informed us that it has established an authorized requestor process for restoring all data files from tape. DIT also informed us that it will establish an internal process to periodically test backup tapes and will continue to work on completing a comprehensive disaster recovery plan for OMNI.

GLOSSARY

Glossary of Acronyms and Terms

access controls

Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.

ADSS

Automated Data Systems Section.

AFIS

national Automated Fingerprint Identification System.

availability

Timely and reliable access to data and information systems.

change controls

Controls that ensure that program, system, and infrastructure modifications are properly authorized, tested, documented, and monitored.

CHRS

Criminal History Records System.

CMIS

Corrections Management Information System.

Control Objectives for Information and Related Technology (CobiT)

A framework, control objectives, and audit guidelines developed by the IT Governance Institute as a generally applicable and accepted standard for good practices for controls over information technology.

data element

A combination of characters or bytes referring to one separate item of information, such as name, address, or age.

DIT

Department of Information Technology.

DOC

Department of Corrections.

effectiveness

Program success in achieving mission and goals.

general controls

The structure, policies, and procedures that apply to an entity's overall computer operations. These controls include an entitywide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls.

information technology (IT)

Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes hardware, software, procedures, services, and related resources.

integrity

Accuracy, completeness, and timeliness of data in an information system.

LEIN

Law Enforcement Information Network.

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.

National Institute of Standards and Technology (NIST)

An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs.

offender

A prisoner, parolee, or probationer.

offender callout

A listing of offender activities for a given day.

OMNI

Offender Management Network Information System.

OMNI user profile

An OMNI application privilege assigned to a user that allows the user to view, enter, edit, or delete records in OMNI.

operating system

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.

OTIS

Offender Tracking Information System.

Parole Board

The sole paroling authority for felony offenders committed to the jurisdiction of the Department of Corrections.

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.

privileged access

Extensive system access capabilities granted to individuals responsible for maintaining system resources. This level of access is considered high risk and must be controlled and monitored by management.

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.

risk assessment

The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Risk assessment is a part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.

segregation of duties

Separation of the management or execution of certain duties or areas of responsibility in order to prevent and reduce opportunities for unauthorized modification or misuse of data or service.

system administrator

The person responsible for installing, configuring, and maintaining the networks, computers, and system security.

warrant

A judicial writ authorizing an officer to make a search, seizure, or arrest or to execute a judgment.

This Page Left Intentionally Blank

STATE OF MICHIGAN

OFFICE of the AUDITOR GENERAL