MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF THE

ACCESSIBLE WEB-BASED ACTIVITY AND REPORTING ENVIRONMENT (AWARE)

DEPARTMENT OF ENERGY, LABOR & ECONOMIC GROWTH AND
MICHIGAN DEPARTMENT OF INFORMATION TECHNOLOGY

March 2009

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

641-0591-08

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

Accessible Web-Based Activity and Reporting Environment (AWARE)

Department of Energy, Labor & Economic Growth (DELEG) and Michigan Department of Information Technology (MDIT)

Report Number:
641-0591-08

Released:
March 2009

AWARE is a case management and payment system used by DELEG's Michigan Rehabilitation Services (MRS) to access data and process payments to help people with disabilities prepare for, find, and keep a job. MDIT provides information support services to DELEG for AWARE, including operating system configuration, application development and maintenance, database administration, production source code and data change controls, and backup and recovery.

Audit Objective:

To assess the effectiveness of DELEG and MDIT's security and access controls over AWARE.

Audit Conclusion:

DELEG and MDIT's security and access controls over AWARE were not effective. We noted two material conditions (Findings 1 and 2) and five reportable conditions (Findings 3 through 7).

Material Conditions:

DELEG and MDIT did not ensure that their practices and methods of sharing confidential MRS customer data with third parties were secure and had not considered whether they should be continued (Finding 1).

MDIT and DELEG had not developed a comprehensive change control process for AWARE (Finding 2).

Reportable Conditions:

MDIT and DELEG did not restrict the database administrator's access to the AWARE application and operating system (Finding 3).

DELEG had not established an information systems security officer position (Finding 4).

MDIT had not fully established effective security controls over the server operating systems (Finding 5).

MDIT and DELEG had not fully established security controls over the AWARE production, test, and reporting databases (Finding 6).

DELEG had not established effective access controls over AWARE (Finding 7).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:

To assess the effectiveness of DELEG's efforts to establish system controls over the processing of data within AWARE.

Audit Conclusion:

DELEG was moderately effective in its efforts to establish system controls over the processing of data within AWARE. We noted three reportable conditions (Findings 8 through 10).

Reportable Conditions:

DELEG had not implemented data edits to ensure the integrity of AWARE data (Finding 8).

DELEG could improve its controls by matching MRS customer data contained in AWARE to other data sources to determine the continued eligibility of customers and, if appropriate, recoup payments (Finding 9).

DELEG did not fully develop and monitor audit trails for AWARE (Finding 10).

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:

Our audit report contains 10 findings and 10 corresponding recommendations. The agency preliminary responses indicate that DELEG and MDIT agree with all of the recommendations and have complied or will comply with them.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Background:

Executive Order No. 2008-20 renamed the Department of Labor and Economic Growth as the Department of Energy, Labor & Economic Growth effective December 28, 2008.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

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

March 10, 2009

Mr. Stanley F. Pruss, Director
Department of Energy, Labor & Economic Growth
Ottawa Building
Lansing, Michigan
and
Mr. Kenneth D. Theis, Director
Michigan Department of Information Technology
George W. Romney Building
Lansing, Michigan

Dear Mr. Pruss and Mr. Theis:

This is our report on the performance audit of the Accessible Web-Based Activity and Reporting Environment (AWARE), Department of Energy, Labor & Economic Growth and Michigan Department of Information Technology.

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 Department of Energy, Labor & Economic Growth and the Michigan Department of Information Technology's 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

ACCESSIBLE WEB-BASED ACTIVITY AND REPORTING ENVIRONMENT (AWARE)
DEPARTMENT OF ENERGY, LABOR & ECONOMIC GROWTH AND
MICHIGAN DEPARTMENT OF INFORMATION TECHNOLOGY

GLOSSARY

Description of System

Michigan Rehabilitation Services (MRS)

MRS provides services to people with disabilities who need vocational rehabilitation services to prepare for, find, and keep a job. MRS serves people in their communities through 35 field offices staffed by rehabilitation counselors. In addition, one or more MRS counselors provide vocational rehabilitation services at each of the 100 Michigan Works! Service Centers*.

MRS was located within the Department of Labor and Economic Growth. Executive Order No. 2008-20 renamed the Department of Labor and Economic Growth as the Department of Energy, Labor & Economic Growth (DELEG) effective December 28, 2008.

Accessible Web-Based Activity and Reporting Environment (AWARE)

AWARE is a case management and payment system designed by a third party contractor for public vocational rehabilitation agencies. MRS staff use AWARE to perform all tasks and access data for customer case management and to process payments. AWARE has 16 modules that each perform a different function in the vocational rehabilitation process. The modules cover the life cycle of a customer from referral and application through eligibility determination, employment plan, customer employment, case closure, and postemployment services. All federally required vocational rehabilitation information is collected and stored in the system. Information stored in AWARE includes customer race, age, disability, social security number, health information, eligibility information, employment plan, progress reports, service authorizations, payment authorizations, and case closure information. Also, MRS staff use AWARE to process payments to customers and vendors who provide rehabilitative services or products. During fiscal year 2006-07, MRS processed expenditures of approximately $39 million using AWARE. MRS provides services to more than 27,000 active customers at any time.

Michigan Department of Information Technology (MDIT)

MDIT provides information support services to DELEG for AWARE, including operating system configuration, application development and maintenance, database administration, production source code and data change controls, and backup and recovery.

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

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit* of the Accessible Web-Based Activity and Reporting Environment (AWARE), Department of Energy, Labor & Economic Growth (DELEG) and Michigan Department of Information Technology (MDIT), had the following objectives:

1. To assess the effectiveness* of DELEG and MDIT's security and access controls over AWARE.

2. To assess the effectiveness of DELEG's efforts to establish system controls over the processing of data within AWARE.

Audit Scope

Our audit scope was to examine the information processing and other records related to the Accessible Web-Based Activity and Reporting Environment (AWARE). We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Our audit procedures, conducted from April through September 2008, generally covered the period January 1, 2000 through September 30, 2008.

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 the security and access controls over AWARE. We obtained an understanding of AWARE controls, including an understanding of the Michigan Rehabilitation Services (MRS) business processes.

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

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 performed an assessment of security and access controls and an assessment of system controls over the processing of data within AWARE. Specifically, we assessed:

a. Security and Access Controls:

(1) We examined and tested user authorization and password controls over AWARE. We obtained an understanding of access policies and procedures. We judgmentally selected 76 active users from the population of 761 active users in AWARE and tested for the existence of authorized user access forms.

(2) We examined and tested user access permissions for AWARE. We interviewed MRS staff and reviewed MRS policies and procedures to obtain an understanding of user access. We judgmentally selected and reviewed the appropriateness of access rights for 29 of 323 active users in AWARE. In addition, we judgmentally selected and reviewed the appropriateness of 23 of 183 users with the ability to authorize payments that exceeded AWARE user security guidelines.

(3) We reviewed and assessed database management and operating system controls.

(4) We reviewed and assessed security management and data security and privacy controls over sharing data with third parties.

(5) We reviewed and evaluated controls over production source code and data changes.

(6) We reviewed and assessed controls over backup and recovery procedures for AWARE.

(7) We reviewed a vulnerability* scan of the network operating systems for AWARE performed by the MDIT Office of Enterprise Security. We evaluated and validated the results of the vulnerability scans and performed additional tests of the operating systems.

b. System Controls Over the Processing of Data:

(1) We interviewed MRS staff to gain an understanding of critical information and processing controls within AWARE. We reviewed AWARE system documentation.

(2) We identified and tested selected data fields within AWARE to determine the accuracy and completeness of data processing controls. We developed tests based on critical information maintained in AWARE, such as customer, case, authorization, and payment information. Our testing included customer cases that were created or active since the implementation of AWARE resulting in 139,672 customer records, 906,702 expenditure transactions, and 715,920 authorization transactions. We also performed a match of MRS data with Department of Corrections prisoner records and Department of Community Health death records to determine the continued eligibility of MRS customers.

(3) We reviewed and evaluated the implementation and use of audit trails within AWARE.

When selecting activities or programs for audit, we use an approach based on assessment of risk and opportunity for improvement. Accordingly, we focus our audit efforts on activities or programs having the greatest probability for needing improvement as identified through a preliminary review. Our limited audit resources are used, by design, to identify where and how improvements can be made. Consequently, we prepare our performance audit reports on an exception basis.

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

Agency Responses

Our audit report contains 10 findings and 10 corresponding recommendations. The agency preliminary responses indicate that DELEG and MDIT agree with all of the recommendations and have complied or 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 DELEG and MDIT 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

SECURITY AND ACCESS CONTROLS

COMMENT

Audit Objective: To assess the effectiveness of the Department of Energy, Labor & Economic Growth (DELEG) and the Michigan Department of Information Technology's (MDIT's) security and access controls over the Accessible Web-Based Activity and Reporting Environment (AWARE).

Audit Conclusion: DELEG and MDIT's security and access controls over AWARE were not effective. Our assessment disclosed two material conditions*. DELEG and MDIT did not ensure that their practices and methods of sharing confidential Michigan Rehabilitation Services (MRS) customer data with third parties were secure and had not considered whether they should be continued (Finding 1). Also, MDIT and DELEG had not developed a comprehensive change control process for AWARE (Finding 2).

Our assessment also disclosed five reportable conditions* related to segregation of duties, security officer, operating system security controls, database security controls, and access controls (Findings 3 through 7).

FINDING

1. Data Security and Privacy Controls

DELEG and MDIT did not ensure that their practices and methods of sharing confidential MRS customer data with third parties were secure and had not considered whether they should be continued. As a result, DELEG and MDIT shared confidential customer data in an insecure manner with third parties.

DELEG electronically provides AWARE customer data to third parties who conduct data analysis services and provides AWARE support and maintenance services. DELEG provides the customer data to the third parties by sending the data over the Internet or by allowing the third parties to access the DELEG network to directly obtain the data.

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

Our review of DELEG and MDIT's controls over providing customer data to third parties disclosed:

a. DELEG and MDIT did not include written data security and privacy requirements within the third party agreements. As a result, DELEG cannot ensure that customer data is appropriately secured by the third parties. The American Institute of Certified Public Accountants' *Generally Accepted Privacy Principles: Principle 7 Disclosure to Third Parties*, which was developed to help entities create a privacy program, states that procedures and controls should be designed to ensure that personal information is disclosed only to third parties that have agreements with the entity to protect personal information from loss, misuse, unauthorized access, disclosure, alteration, and destruction. DELEG and MDIT should seek legal counsel to help review and amend the third party agreements to include confidentiality agreements, data protection requirements, data disposal guidelines, and procedures that the third parties should follow in the event that customer data is compromised.

b. MDIT, in conjunction with DELEG, did not adequately secure customer data before electronically providing the customer data to the third parties. Title 34, Part 361, section 38 of the *Code of Federal Regulations* states that vocational rehabilitation services programs must adopt and implement written policies and procedures to safeguard all confidential personal information. DELEG should secure data by encryption or other methods or remove the customer's personal identification information, such as name, address, date of birth, and social security number. DELEG informed us that the data sharing process included encrypting customer data for one of the third parties. However, our review disclosed that MDIT did not always encrypt the data before sharing it with the third party.

c. DELEG, in conjunction with MDIT, did not verify that the third parties implemented DELEG's security requirements. As a result, DELEG was unaware whether the third parties had implemented adequate security controls over customer data. Title 34, Part 361, section 38 of the *Code of Federal Regulations* states that vocational rehabilitation services programs must have assurances and safeguards over confidential data when data is released to other entities for audit, evaluation, or research purposes. Verification of data

protection from the third parties may include an auditor's report or other representation from the third parties.

After we brought this matter to management's attention, DELEG immediately contacted the third parties to identify and clarify what processes are in place to share and secure customer data. However, DELEG should continue to work with the third parties and MDIT to strengthen agreements and implement data security and privacy controls over customer data.

RECOMMENDATION

We recommend that DELEG and MDIT ensure that their practices and methods of sharing confidential MRS customer data with third parties are secure and consider whether they should be continued.

AGENCY PRELIMINARY RESPONSE

DELEG and MDIT agree and informed us that MDIT has worked closely with DELEG leadership to ensure that services are technologically sound, secure, and cost effective. MDIT also informed us that it will continue to reduce the risk to State computer systems by implementing effective internal control to safeguard all confidential personal information. In addition, MDIT informed us that it has not identified any instances of lost or stolen personal information as a result of a security breach of AWARE.

Regarding part a., DELEG and MDIT informed us that they are working in conjunction with the Department of Management and Budget to amend the current contract to include data security and privacy requirements. DELEG and MDIT also informed us that they will protect personal information by documenting procedures to enforce current security policies that require information only be disclosed to third parties that have agreements with the State.

Regarding part b., DELEG and MDIT informed us that they will implement formal procedures to adequately secure customer data and utilize encryption and secure transmission protocols to electronically provide customer data to third parties.

Regarding part c., DELEG informed us that one of the third party vendors currently provides formal documentation attesting that ethics training and human subject confidentiality agreements are in place prior to allowing authorized individuals

access to AWARE customer data. MDIT informed us that it will work with DELEG to formally document procedures requiring the monitoring of third party security controls over customer data.

FINDING

2. Change Control Process

MDIT and DELEG had not developed a comprehensive change control process for AWARE. As a result, MDIT and DELEG could not ensure that the production source code and data changes were properly controlled to ensure protection from unauthorized changes.

Control Objectives for Information and Related Technology* (COBIT) states that managing changes helps minimize the likelihood of disruption, unauthorized alterations, and errors. Managing changes is accomplished by instituting policies, procedures, and techniques to help ensure that all production source code and data changes are properly requested, authorized, tested, approved, and logged and that access to production source code and data is controlled. Our review disclosed:

a. MDIT and DELEG had not established documented change control policies and procedures. Change control policies and procedures should define the process for requesting, approving, implementing, logging, and testing program and data changes. Also, policies and procedures should define the process for conducting emergency changes. In addition, policies and procedures should establish controls over segregation of duties* for moving source code in and out of the production environment. The use of policies and procedures helps ensure that management's intent is clearly communicated to all individuals responsible for production source code and data change controls.

b. MDIT and DELEG did not use a standardized change request form. MDIT informed us that production source code and data change requests are initiated verbally or by e-mail. The use of a standardized form helps ensure that all requests are clearly communicated and approvals are documented.

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

c. MDIT and DELEG did not maintain a complete log of production source code and data changes. MDIT maintains a log of production source code changes and data changes made directly to the data without using an AWARE user account. However, the log did not include all of the changes and did not include evidence of user acceptance testing, approvals, and who implemented the change. A complete log of program changes would help to ensure that production source code and data changes are authorized and approved by management.

d. MDIT had not established effective controls to ensure the integrity* of production source code versions. As a result, MDIT could move an older version of production source code back into production that could cause AWARE to not work as intended. CobiT states that a software release process helps to ensure proper version control. Library control software is often used to provide production source code version controls. Library control software provides a mechanism for developers to check in and check out production source code and provides a means for management to log and monitor when a source code is copied or changed.

RECOMMENDATION

We recommend that MDIT and DELEG develop a comprehensive change control process for AWARE.

AGENCY PRELIMINARY RESPONSE

MDIT and DELEG agree and informed us that MDIT has a comprehensive change management process and has developed formal procedures to include all change management processes. DELEG informed us that it will comply with MDIT's comprehensive change control process and will also implement an internal change tracking log for DELEG's AWARE Support Unit. In addition, MDIT informed us that it is evaluating cost-effective methods to implement library control software to maintain a list of changes and versions for AWARE.

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

FINDING

3. Segregation of Duties

MDIT and DELEG did not restrict the database administrator's access to the AWARE application and operating system. As a result, the database administrator could circumvent system controls and process unauthorized transactions and service payments.

CobiT states that proper segregation of duties helps to reduce the risk of a single individual bypassing critical controls and helps to reduce the risk of inadvertent or intentional processing of unauthorized transactions. Segregation of duties also helps to reduce the risk of implementing improper production source code or data changes.

The AWARE database administrator had unnecessary access rights to the AWARE application and operating system, including multiple user accounts with privileged access* to AWARE and administrative access rights to the operating system. Having multiple user accounts allows a single user to authorize and approve payments. Also, having privileged access to AWARE allows the database administrator the ability to create, delete, and modify user access rights for any user account. In addition, having administrative access rights to the operating system could allow the database administrator to commit fraudulent activity that would likely go undetected, such as copying and selling confidential information or inserting a malicious code into the application. Our review did not disclose any instances of fraudulent activities.

After we brought this matter to management's attention, MDIT removed the database administrator's access to the operating system and DELEG removed the database administrator's privileged access to AWARE.

RECOMMENDATION

We recommend that MDIT and DELEG restrict the database administrator's access to the AWARE application and operating system.

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

AGENCY PRELIMINARY RESPONSE

MDIT and DELEG agree and informed us that they have complied. Also, MDIT informed us that, immediately upon notification of the finding, MDIT removed the database administrator's access to the operating system and DELEG removed administrator privileged access to AWARE.

FINDING

4. Security Officer

DELEG had not established an information systems security officer position. Without an information systems security officer, management cannot effectively address security weaknesses and maintain the integrity and availability of information systems and data.

The National Institute of Standards and Technology* (NIST) states that security officer duties should include facilitating risk assessments*, monitoring compliance with security policies, educating users about the importance of data security, and advising senior management on security policy related issues. DELEG's lack of a security officer may have contributed to, or left uncorrected, several weaknesses that we noted during the course of our audit, such as the lack of user access and data security controls.

RECOMMENDATION

We recommend that DELEG establish an information systems security officer position.

AGENCY PRELIMINARY RESPONSE

DELEG agrees and informed us that it will comply. DELEG informed us that it recently assigned the security officer responsibilities to an individual who also serves as its internal control officer. DELEG also informed us that the security officer will work with DELEG and MDIT management to establish departmentwide standards and procedures to ensure the integrity and availability of DELEG information systems and data. In addition, DELEG informed us that monitoring for compliance with standards and procedures will be conducted during DELEG's biennial evaluation process and on an ongoing basis.

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

FINDING

5. Operating System Security Controls

MDIT had not fully established effective security controls over the server operating systems*. As a result, MDIT could not ensure that AWARE data was protected from unauthorized modification, loss, or disclosure.

A well-secured operating system would help provide a stable platform on which to run DELEG's information systems, such as AWARE. MDIT procedure 1350.11 requires the secure establishment, maintenance, and administration of servers, including operating system software and the data residing on the servers. Operating system security controls should be established to protect information and resources from unauthorized modification, loss, or disclosure by restricting or detecting inappropriate access attempts. In addition, an operating system should be installed with a minimal service configuration to reduce the risk of network intrusion and exploitation of well-known operating system vulnerabilities.

Our review of nine servers that contained the databases and Web servers for AWARE identified vulnerable operating system configurations on all nine servers. Because of the confidentiality of operating system configurations, we summarized the results of our testing for presentation in this finding and provided the detailed results to MDIT.

After we brought this matter to management's attention, MDIT informed us that it began taking steps to correct the weaknesses.

RECOMMENDATION

We recommend that MDIT fully establish effective security controls over the server operating systems.

AGENCY PRELIMINARY RESPONSE

MDIT agrees and informed us that it has complied. MDIT also informed us that it is committed to strengthening security controls over the server operating systems. In addition, MDIT informed us that all server security exceptions have been addressed and server security now meets industry best practice recommendations.

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

FINDING

6. Database Security Controls

MDIT and DELEG had not fully established security controls over the AWARE production, test, and reporting databases. Fully establishing database security controls would help prevent or detect inappropriate access to AWARE data.

According to ISO/IEC 27002:2005*, *Information technology - Security techniques - Code of Practice for Information Security Management*, a well-secured database provides a protected environment to maintain the integrity and confidentiality of data. Appropriate security controls include using individual user accounts and passwords, monitoring to ensure that users are performing only the activities which they are explicitly authorized to perform, and using audit logs to record and monitor significant events. Our review of the 3 AWARE databases disclosed:

a. MDIT did not fully restrict certain users from having privileged access rights to 1 of the 3 databases. We reviewed 23 database users and identified 4 users with excessive access rights to the production database. After we brought this matter to management's attention, MDIT removed 2 of the 4 user accounts from the database. However, DELEG believed that the other 2 users should continue to have the privileged access in order to create federal reports.

b. MDIT did not remove user accounts for individuals who no longer required access to 1 of the 3 databases. We identified 10 active user accounts belonging to users who no longer required access to the production database. After we brought this matter to management's attention, MDIT removed the 10 user accounts from the database.

c. MDIT had not established unique user accounts and passwords for all database users on 1 of the 3 databases. We noted that 4 MDIT staff shared a single database user account. Establishing unique user accounts and passwords would help ensure that users perform only those duties that management authorized them to perform. After we brought this matter to management's attention, MDIT removed the shared user account from the database.

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

d. MDIT did not use database audit logs to monitor database administrator activity on all 3 databases. Audit logs can be configured to record privileged access and identify unusual or unauthorized activity. MDIT informed us that continuously running the audit logs on its database would negatively impact performance. However, the recording and monitoring of selected high-risk events would help to enhance database security.

e. MDIT had not implemented sufficient controls over database passwords on all 3 databases. As a result, MDIT did not require technical staff to use alphanumeric characters in their passwords or periodically change their passwords after a specific period of time. MDIT procedure 1310.03 states that passwords should contain a combination of alphanumeric and nonalphanumeric characters. Requiring passwords to include alphanumeric characters and changing passwords on a regular basis helps to ensure password confidentiality and reduces the risk of unauthorized access to the system.

f. MDIT, in conjunction with DELEG, did not encrypt AWARE data on all 3 databases. Encryption is a method used to change data into an unreadable format. MDIT policy 1340 states that sensitive data, such as name, social security number, and health information, should be encrypted. Encryption would help to ensure that confidential data in AWARE (such as customer name, address, and date of birth; social security numbers; and customer health information) is protected from unauthorized disclosure.

g. MDIT, in conjunction with DELEG, had not developed a complete data dictionary for the AWARE database. As a result, DELEG could not ensure that it maintained data integrity and minimized data redundancy. A data dictionary contains detailed information about data, including a definition and acceptable values for each data element*.

RECOMMENDATION

We recommend that MDIT and DELEG fully establish security controls over the AWARE production, test, and reporting databases.

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

AGENCY PRELIMINARY RESPONSE

MDIT and DELEG agree and MDIT informed us that it and DELEG have already taken steps to strengthen database security controls over AWARE and expect full compliance by June 1, 2009.

Regarding part a., MDIT informed us that it removed users with excessive access rights. MDIT also informed us that it will monitor, control, and document staff access to the production database.

Regarding part b., MDIT informed us that it removed developers with excessive access rights.

Regarding parts c. and e., MDIT informed us that database security controls now meet industry best practice recommendations and MDIT security policies.

Regarding part d., MDIT informed us that it is continuously working with the clients to improve security and performance. MDIT also informed us that it is currently working with an external group to monitor performance measures and reduce risk to AWARE. MDIT further informed us that an analysis of automated audit logs of high level events will be performed.

Regarding part f., MDIT informed us that it will work with the contractor to encrypt AWARE data on all three databases and comply with MDIT policy 1340.

Regarding part g., MDIT informed us that it will develop a data dictionary for AWARE tables.

FINDING

7. Access Controls

DELEG had not established effective access controls over AWARE. Without effective access controls, DELEG cannot ensure the security and integrity of AWARE data.

CobiT states that access controls help to ensure that access to systems and data is restricted to authorized users and that data is safeguarded from unauthorized use,

disclosure, modification, damage, or loss. Our review of access and password controls over AWARE disclosed the following weaknesses:

a. DELEG had not implemented strong password policies in AWARE. Specifically, DELEG did not require users to use a password containing 7 characters and a combination of alphanumeric, uppercase, lowercase, and nonalphanumeric characters. MDIT procedure 1310.03 states that the minimum industry standard password length is 7 characters and that passwords should contain a combination of alphanumeric and nonalphanumeric characters.

b. DELEG did not restrict the ability to create, modify, and delete users' access rights in AWARE to appropriate individuals. As a result, one user could inadvertently or intentionally grant themselves or others inappropriate and unauthorized access rights in AWARE. We noted that one DELEG employee was granted this ability who did not have a business need to create, modify, and delete users. After we brought this matter to management's attention, DELEG removed the access right from the user's account.

c. DELEG did not monitor users' failed log-ins or multiple log-ins to AWARE. ISO/IEC 27002:2005 (E) states that audit logs should be implemented and maintained to selectively identify unauthorized, unusual, and sensitive user activities, such as attempted unauthorized access.

d. DELEG did not restrict MDIT developer and third party contractor access to AWARE. We noted 5 MDIT developers and 6 third party contractors with access to AWARE. As a result, these individuals could access confidential and sensitive information and change data without DELEG's authorization or knowledge. After we brought this matter to management's attention, DELEG removed the user accounts for 2 MDIT developers and 3 third party contractors and changed the access rights to "read only" for 3 MDIT developers and 3 third party contractors.

e. DELEG did not appropriately assign user access rights based on AWARE user security guidelines. The AWARE user security guidelines include a matrix and user access authorization form that outlines the type of access individuals should be granted based upon their job roles and responsibilities. We

judgmentally selected and reviewed access rights assigned to 29 MRS district and site managers, rehabilitation assistants, and blended staff*. We noted that 11 (38%) of the 29 individuals had inappropriate access rights. After we brought this matter to management's attention, DELEG removed the inappropriate access rights for 10 of the 29 individuals and approved access for 1 individual.

f. DELEG did not restrict payment authorization access rights of MRS staff for processing service payments in AWARE. MRS staff have authorized dollar limits for drafting, issuing, and approving service payments. We identified 183 users with the ability to process AWARE payments in excess of the users' authorized dollar limits. We judgmentally selected and tested 23 of 183 users for which the user's authorized dollar amount exceeded the appropriate limit based on AWARE user security guidelines. We noted that 6 of the 23 users did not have management's approval to exceed the defined dollar limit.

RECOMMENDATION

We recommend that DELEG establish effective access controls over AWARE.

AGENCY PRELIMINARY RESPONSE

DELEG agrees and informed us that it will comply. DELEG also informed us that it will implement strong passwords, log-in audit logs, monitoring, and stronger quarterly reviews of user access by June 1, 2009. In addition, DELEG informed us that user access rights have been corrected. Further, DELEG informed us that DELEG staff independent of the AWARE process will perform semiannual reviews of access and related rights granted to MRS staff.

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

SYSTEM CONTROLS OVER THE PROCESSING OF DATA

COMMENT

Audit Objective: To assess the effectiveness of DELEG's efforts to establish system controls over the processing of data within AWARE.

Audit Conclusion: DELEG was moderately effective in its efforts to establish system controls over the processing of data within AWARE. Our assessment disclosed three reportable conditions related to data processing controls, data matches, and audit trails (Findings 8 through 10).

FINDING

8. Data Processing Controls

DELEG had not implemented data edits to ensure the integrity of AWARE data. Without data edits, inaccurate or missing information could affect the accuracy of MRS customer records.

Data edits would help ensure complete data processing and the integrity of data throughout the MRS customer rehabilitation process.

For parts a. and b. of this finding, we tested 906,702 customer expenditures in AWARE. For part c., we tested 715,920 authorizations in AWARE. Although there was not a large number of exceptions, these edits should be in place as part of DELEG's system of internal control over service payments. Our review of AWARE data disclosed:

a. DELEG did not ensure that AWARE contained edits to prohibit recurring payments* from exceeding $500 per day. MRS policy 9225 states that recurring payments to a customer cannot exceed $500 per day. We identified 573 recurring payments that were greater than $500 per day. The payments ranged from $504 to $16,000 for a total of approximately $485,000.

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

b. DELEG did not ensure that AWARE contained edits to reject payments that exceeded the authorized service amounts. MRS policy 9200 states that a case note shall document the reason for a payment exceeding the authorized service amount by the greater of $10 or 10% of the original authorization. We identified 3 payments that exceeded the authorized service amount by $20, $49, and $1,965. We reviewed the case notes for the 3 payments and did not find an explanation for the payments exceeding the authorized service amounts.

c. DELEG did not ensure that AWARE contained edits to reject invalid service authorization date and service period date combinations. MRS staff authorize a period of time in which customers may receive services that help the customers reach their employment goal. We identified 129 service authorizations for which the end date of the service period was before the beginning date of the service period. We also identified 3,836 authorized services for which the service end date was prior to the date that the service was authorized, by giving the appearance of a retroactive payment. MRS policy 9175 states that retroactive payments occur when an authorization for service is issued after the service is provided. MRS policy 9175 also states that retroactive authorizations are prohibited unless prior written or verbal approval was given to the service provider by MRS.

RECOMMENDATION

We recommend that DELEG implement data edits to ensure the integrity of AWARE data.

AGENCY PRELIMINARY RESPONSE

DELEG agrees and informed us that it will comply. DELEG also informed us that recurring payments exceeding $500 will be prohibited by data edits effective April 1, 2009. In addition, DELEG informed us that payments exceeding parameters have not occurred since November 2007 and that controls are in place to immediately identify any payments exceeding parameters so that diagnosis can occur. DELEG further informed us that invalid service authorization dates and service date combinations last occurred in June 2008, prior to the code correction.

FINDING

9. Data Matches

DELEG could improve its controls by matching MRS customer data contained in AWARE to other data sources to determine the continued eligibility of customers and, if appropriate, recoup payments. Matching AWARE data to other data sources would help detect or prevent payments to incarcerated and deceased customers.

The mission* of MRS includes partnering with individuals and employers to achieve quality employment outcomes and independence for persons with disabilities. MRS policy 5025 states that customer employment outcomes should be consistent with the customer's strengths, resources, priorities, concerns, abilities, capabilities, and interests. Incarcerated and deceased individuals would not be capable of achieving quality employment outcomes and independence because they are unable to obtain employment.

We matched customer social security numbers with Department of Corrections (DOC) prisoner records. We also matched customer social security numbers, names, and birth dates with the Department of Community Health death records. Our testing of 139,672 active customer cases disclosed:

a. DELEG issued inappropriate payments for 6 customers for services dated while the customers were incarcerated in prison. Payments for these individuals totaled $1,415. DELEG issued the payments to 4 customers and 2 vendors totaling $127 and $1,287, respectively. Matching customer data to DOC prisoner records would help DELEG avoid costs for incarcerated individuals.

b. DELEG did not maintain complete customer files to document the appropriateness of payments for 4 customers. We reviewed the 4 customers' case files and could not determine if the customer was incarcerated at the time of service because the case file lacked complete documentation, such as missing or incomplete service authorization forms. DELEG issued payments totaling $1,254 for the 4 customers.

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

c. DELEG issued payments for 21 deceased customers totaling $9,157. The payments were made for services dated after the customers were deceased. DELEG issued the payments to the customers or to vendors for a total of $60 and $9,097, respectively. Payments to 20 of the 21 deceased customers were cashed.

RECOMMENDATION

We recommend that DELEG match MRS customer data contained in AWARE to other data sources to determine the continued eligibility of customers and, if appropriate, recoup payments.

AGENCY PRELIMINARY RESPONSE

DELEG agrees and informed us that it will comply. DELEG also informed us that it will consider matching customers to other data sources after ensuring the confidentiality of DELEG customer information and its ability to acquire agreements associated with data security and privacy controls with other data sources. In addition, DELEG informed us that a cost-benefit analysis and other logistical considerations will be assessed prior to deciding to implement this control.

FINDING

10. Audit Trails

DELEG did not fully develop and monitor audit trails for AWARE. Without an audit trail, it is difficult to prove accountability for transactions and to ensure the reliability and accuracy of customer service payments.

NIST Audit Trails Security Bulletin 97-03 states that recording user activities can help maintain accountability and reconstruct events after a problem has occurred. DELEG recorded the usercode of the person who last updated a record; however, DELEG did not fully include a history of all changes. We noted four data fields that DELEG captured in an audit log that included a history of changes. However, logging sensitive transactions, such as customer address changes and payments, on closed cases would enable DELEG to identify the user who made the change in the event of questionable transactions.

DELEG informed us that during September 2008 it would implement a new version of AWARE which includes additional audit trail functionality. DELEG also informed

us that the new audit trail functionality includes logging changes to data fields, such as customer name, address, social security number, and customer budget information.

RECOMMENDATION

We recommend that DELEG fully develop and monitor audit trails for AWARE.

AGENCY PRELIMINARY RESPONSE

DELEG agrees and informed us that it will comply. DELEG also informed us that a new version of AWARE (5.0) will contain significant audit functionality and will be fully implemented by March 1, 2009. In addition, DELEG informed us that it is working with MDIT Vantage Enterprise Group and will implement this functionality incrementally.

GLOSSARY

Glossary of Acronyms and Terms

AWARE	Accessible Web-Based Activity and Reporting Environment.
blended staff	Rehabilitation and clerical staff who are employed by an MRS community partner. Blended staff, under formal written arrangements, perform some of the same duties as their MRS counterparts in MRS offices. Blended staff are under the direct supervision of a local MRS site manager, who is a State employee.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines published 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.
DELEG	Department of Energy, Labor & Economic Growth.
DOC	Department of Corrections.
effectiveness	Program success in achieving mission and goals.
integrity	Accuracy, completeness, and timeliness of data in an information system.
ISO/IEC 27002:2005	A security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) that establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in the standard provide general guidance on the commonly accepted goals of information security management.

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.
MDIT	Michigan Department of Information Technology.
Michigan Works! Service Centers	DELEG's Michigan Works! Service Centers are locations where a wide range of employment, training, and career education services are available to the public.
mission	The main purpose of a program or agency or the reason that the program or agency was established.
MRS	Michigan Rehabilitation Services.
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.
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 program operations, to facilitate decision making by parties responsible for overseeing or initiating corrective action, and to improve accountability.
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.
recurring payment	A payment to an individual for weekly, biweekly, or monthly checks.

reportable condition	A matter that, in the auditor's judgment, falls within any of the following categories: an opportunity for improvement within the context of the audit objectives; a deficiency in internal control that is significant within the context of the objectives of the audit; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely to have occurred.
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.
server operating system	The software that manages the application and data files that are shared over a network.
vulnerability	Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL