MICHIGAN

OFFICE OF THE AUDITOR GENERAL

FOLLOW-UP REPORT
ON THE

ACCESSIBLE WEB-BASED ACTIVITY AND REPORTING ENVIRONMENT (AWARE)

DEPARTMENT OF HUMAN SERVICES AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

November 2013

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

641-0591-08F

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

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

November 8, 2013

Ms. Maura D. Corrigan, Director
Department of Human Services
Grand Tower
Lansing, Michigan
and
John E. Nixon, C.P.A., Director
Department of Technology, Management, and Budget
George W. Romney Building
Lansing, Michigan
and
Mr. David B. Behen, Chief Information Officer
Department of Technology, Management, and Budget
Lewis Cass Building
Lansing, Michigan

Dear Ms. Corrigan, Mr. Nixon, and Mr. Behen:

This is our report on our follow-up of the 2 material conditions (Findings 1 and 2) and 2 corresponding recommendations reported in the 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). That audit report was issued and distributed in March 2009. Additional copies are available on request or at <http://audgen.michigan.gov>.

In March 2010, subsequent to our performance audit, Executive Order No. 2009-55 renamed the Department of Management and Budget as the Department of Technology, Management, and Budget (DTMB). It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and unexpended balances of appropriations, allocations, or other funds of MDIT to DTMB and abolished MDIT. Also, in October 2012, Executive Order No. 2012-10 transferred all of the authority, powers, duties, functions, records, personnel, property, and unexpended balances of appropriations, allocations, or other funds of Michigan Rehabilitation Services to the Department of Human Services (DHS).

This report contains an introduction, our purpose of follow-up, a background, our scope, follow-up conclusions and results, and a glossary of acronyms and terms.

Our follow-up disclosed that DHS and DTMB had complied with both recommendations.

If you have any questions, please call me or Scott M. Strong, C.P.A., C.I.A., Deputy Auditor General.

Sincerely,

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

This Page Left Intentionally Blank

TABLE OF CONTENTS

FOLLOW-UP REPORT
ACCESSIBLE WEB-BASED ACTIVITY AND REPORTING ENVIRONMENT (AWARE)
DEPARTMENT OF HUMAN SERVICES AND
DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

FOLLOW-UP REPORT
ACCESSIBLE WEB-BASED ACTIVITY AND REPORTING ENVIRONMENT (AWARE)
DEPARTMENT OF HUMAN SERVICES AND DEPARTMENT OF TECHNOLOGY, MANAGEMENT, AND BUDGET

INTRODUCTION

This report contains the results of our follow-up of the material conditions* and corresponding recommendations reported in 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), 641-0591-08, which was issued and distributed in March 2009. That audit report included 2 material conditions (Findings 1 and 2) and 8 reportable conditions*. This report also contains DELEG's and MDIT's plans to comply with our prior audit recommendations for the 2 material conditions, which were required by the *Michigan Compiled Laws* and administrative procedures to be developed within 60 days after release of the March 2009 audit report.

PURPOSE OF FOLLOW-UP

The purpose of this follow-up was to determine whether the Department of Human Services (DHS) and the Department of Technology, Management, and Budget (DTMB) had taken appropriate corrective measures in response to the 2 material conditions and 2 corresponding recommendations noted within our March 2009 audit report.

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

BACKGROUND

Michigan Rehabilitation Services (MRS)

MRS provides services to people with disabilities who need vocational rehabilitation to prepare for, find, and keep a job. MRS rehabilitation counselors serve customers from over 30 field offices. MRS counselors provide a presence in all 83 counties by also meeting with customers in Michigan Works! Agencies* and DHS offices Statewide.

At the time of the performance audit, MRS was located within DELEG. Executive Order No. 2011-4 renamed DELEG as the Department of Licensing and Regulatory Affairs (LARA) effective in April 2011. Executive Order No. 2012-10 transferred all of the authority, powers, duties, functions, records, personnel, property, and unexpended balances of appropriations, allocations, or other funds of MRS from LARA to DHS effective in October 2012.

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 AWARE. 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.

Department of Technology, Management, and Budget (DTMB)

DTMB provides information support services to DHS 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.*

Executive Order No. 2009-55 renamed the Department of Management and Budget as DTMB effective in March 2010. It also transferred all of the authority, powers, duties, functions, responsibilities, records, personnel, property, equipment, and unexpended balances of appropriations, allocations, or other funds of MDIT to DTMB and abolished MDIT.

SCOPE

Our fieldwork was performed during August and September 2013. To determine the status of compliance with our audit recommendations, we interviewed DHS and DTMB staff. We identified the third parties with whom DHS shared confidential MRS customer data as of the time of our follow-up. We obtained the contracts between DHS and the third parties and the third parties' confidentiality agreements. We assessed DHS and DTMB's practices and methods of sharing confidential MRS customer data with the third parties to determine whether the practices and methods were secure. We also reviewed the efforts of DHS and DTMB to develop a comprehensive change control process for AWARE. We assessed the change control processes in place for source code and data change requests. We judgmentally selected change requests to determine whether the standardized log and change control processes were in place.

FOLLOW-UP CONCLUSIONS AND RESULTS

SECURITY AND ACCESS CONTROLS

SUMMARY OF THE MARCH 2009 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 provide 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.

RECOMMENDATION (AS REPORTED IN MARCH 2009)

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 PLAN TO COMPLY*

The *Michigan Compiled Laws* and administrative procedures required DELEG and MDIT to develop a plan to comply with our audit recommendations within 60 days of the release of the March 2009 audit report. DELEG and MDIT indicated in their 2009 plans to comply that they intended to comply with the recommendation and informed us that MDIT had worked closely with DELEG leadership to ensure that services were technologically sound, secure, and cost-effective. The plans stated that MDIT would continue to reduce the risk to State computer systems by implementing effective internal controls to safeguard all confidential personal information. The plans also stated that MDIT had not identified any instances of lost or stolen personal information as a result of a security breach for DELEG's AWARE system.

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

Specifically, DELEG and MDIT reported the following in their agency plans to comply:

a. Regarding part a. of the original finding, DELEG and MDIT will work in conjunction with the Department of Management and Budget (now DTMB) to amend the current contract to include data security and privacy requirements. DELEG is also in the process of amending its university vendor contract to address the requirements. In addition, DELEG and MDIT 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.

b. Regarding part b. of the original finding, MDIT, in conjunction with DELEG, will implement formal procedures to manage the data sharing process. To adequately secure customer data, the departments are utilizing encryption and secure transmission protocols to electronically provide customer data to third parties.

c. Regarding part c. of the original finding, DELEG third party vendors currently provide formal documentation attesting that ethics training and human subject confidentiality agreements are in place prior to allowing authorized individuals access to AWARE data. MDIT will work in conjunction with DELEG to formally document procedures requiring the monitoring of third party security controls over customer data.

FOLLOW-UP CONCLUSION

DHS and DTMB complied with the recommendation.

FOLLOW-UP RESULTS

DHS and DTMB implemented processes to ensure that their practices and methods of sharing confidential MRS customer data with third parties were secure. With regard to part a. of the original finding, DHS and DTMB included privacy language in the third party contracts that were in place in 2013. In addition, DHS and DTMB established confidentiality agreements which were signed by the third party users of AWARE.

With regard to part b. of the original finding, DTMB created a data sharing policy. Also, DTMB adequately secured data through the use of data scrambling. The data scrambling process replaces the confidential social security numbers with randomly assigned numbers and randomizes the names and addresses that are stored within AWARE. We verified that DTMB followed its policy and adequately secured data prior to sending AWARE data to a third party.

With regard to part c. of the original finding, DHS and DTMB did not require third party contractors to verify that they implemented security requirements. However, because of the implementation of the data scrambling controls noted in the preceding paragraph, DHS and DTMB no longer share confidential customer data with third parties.

SUMMARY OF THE MARCH 2009 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.

RECOMMENDATION (AS REPORTED IN MARCH 2009)

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

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

AGENCY PLAN TO COMPLY

DELEG and MDIT indicated in their 2009 plans to comply that they intended to comply with the recommendation. MDIT had informed DELEG that it now had a comprehensive change management process and had developed formal procedures to include all change management processes. DELEG indicated that it would comply with the MDIT comprehensive change control process and would implement a similar internal system for the AWARE Support Unit.

FOLLOW-UP CONCLUSION

DHS and DTMB complied with the recommendation.

FOLLOW-UP RESULTS

DHS and DTMB developed a comprehensive change control process for AWARE. With regard to part a. of the original finding, MRS developed a change control policy and procedure in June 2009. In addition, DTMB established a change control policy that defined the standard and emergency change control processes. We verified that a comprehensive change control process had been implemented.

With regard to part b. of the original finding, DHS developed an information technology maintenance request form that it submits to DTMB for program changes. In addition, DTMB developed an internal tracking system for program change requests. We verified that the form was being utilized and that the change request process was being followed.

With regard to part c. of the original finding, DHS developed a change management database that contains MRS changes to AWARE. In addition, DTMB internally tracks change requests using a monitoring system. We verified that changes made were included in the DHS database and the DTMB monitoring system.

With regard to part d. of the original finding, we determined that DTMB revised the process for how it makes changes to production programs. DTMB informed us that it receives executable files from the vendor and that these files would not benefit from a library control software system. Based on our review of the change control process and DHS's and DTMB's compliance with parts a. through c. of the original finding, we determined that the absence of library control software was no longer a reportable condition.

Glossary of Acronyms and Terms

agency plan to comply	The response required by Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100). The audited agency is required to develop a plan to comply with Office of the Auditor General audit recommendations and submit the plan within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.
AWARE	Accessible Web-Based Activity and Reporting Environment.
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.
DELEG	Department of Energy, Labor & Economic Growth.
DHS	Department of Human Services.
DTMB	Department of Technology, Management, and Budget.
LARA	Department of Licensing and Regulatory Affairs.
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! Agencies	The local agencies that administer the day-to-day operations of local workforce development programs and services.
MRS	Michigan Rehabilitation Services.
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.
reportable condition	A matter that, in the auditor's judgment, is less severe than a material condition and 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 audit objectives; 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.

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL