JENNIFER M. GRANHOLM
GOVERNOR

STATE OF MICHIGAN
DEPARTMENT OF ENERGY, LABOR & ECONOMIC GROWTH
LANSING

STANLEY "SKIP" PRUSS
DIRECTOR

emailed 7/23/09 (ael)

July 23, 2009

Mr. Doug Ringler, Director
Office of Internal Audit Services
Department of Management & Budget
Romney Building – Seventh Floor
111 S. Capitol, P.O. Box 30026
Lansing, Michigan 48909

Dear Mr. Ringler:

We are enclosing our response to comments made in the Office of the Auditor General's Performance Audit of the Accessible Web-Based Activity and Reporting Environment (AWARE), Department of Energy, Labor and Economic Growth (DELEG) and Michigan Department of Information Technology (MDIT) for the period January 1, 2000 through September 30, 2008. MDIT will be responding to Finding 5 as it was addressed only to that department. Findings 1, 2, 3 and 6 of the report represent findings directed at both departments. These will be addressed by each department separately.

Questions regarding the summary table or corrective action plans should be directed to my attention at 636-0287.

Sincerely,

(SIGNED)

Allen Williams, Director
Office of Audit & Financial Compliance

Enclosure
cc: Audit Distribution List
Stanley Pruss
Andy Levin
Jaye Shamsiddeen
Susan Corbin
Allan Pohl

OFFICE OF AUDIT & FINANCIAL COMPLIANCE
GENERAL OFFICE BUILDING—1ST FLOOR, A-WING • P.O. BOX 30643 • LANSING, MICHIGAN 48909
www.michigan.gov • (517) 636-0229 • TTY 1-888-605-6722

OAG Audit Response Distribution List

Executive Office	Coffiann Hawthorne
Office of the Auditor General	Michael Becker
Senate Fiscal Agency	Gary Olson
House Fiscal Agency	Mitchell E. Bean
Senate Appropriations Committee	Senator Ron Jelinek
House Appropriations Committee	Rep. George Cushingberry Jr.
House Education Committee	Rep. Tim Melton
House New Economy & Quality of Life Committee	Rep. Ed Clemente
House Labor Committee	Rep. Steven Lindberg
Senate Education Committee	Senator Wayne Kuipers
Senate Economic Development and Regulatory Reform Committee	Senator Alan Sanborn
Senate Families and Human Services Committee	Senator Mark Jansen
Michigan Department of Information Technology	Tina Richardson
Department of Management & Budget	John Juarez

AUDIT RESPONSE SUMMARY

Accessible Web-Based Activity and Reporting Environment (AWARE)
Department of Energy, Labor and Economic Growth (DELEG)
(January 1, 2000 through September 30, 2008)

I. Citations complied with:

#3
#4

II. Citations to be complied with:

#1 – Expected date of compliance is December 31, 2009
#2 – Expected date of compliance is December 31, 2009
#6 – Please reference DIT response for the expected date of compliance.
#7 – Expected date of compliance is October 31, 2009
#8 – Expected date of compliance is October 1, 2009
#9 – Expected date of (conditional) compliance is April 30, 2010
#10 – Expected date of compliance is October 1, 2009

III. Citations agency disagrees with:

None

Performance Audit of
Accessible Web-Based Activity and Reporting Environment (AWARE)
Agency Response

1. Data Security and Privacy Controls

DELEG and MDIT did not assess whether the practice and methods of sharing confidential MRS customer data with third parties is secure and should be continued. Specifically:

a. *DELEG and MDIT did not include written data security and privacy requirements within the third party agreements.*
b. *MDIT, in conjunction with DELEG, did not adequately secure customer data, before electronically providing the customer data to the third parties.*
c. *DELEG, in conjunction with MDIT, did not verify that the third parties implemented DELEG's security requirements.*

Agency Response: DELEG agrees with the finding.

MDIT has worked closely with DELEG leadership to ensure that services are technologically sound, secure and cost-effective. MDIT will continue to reduce the risk to state computer systems by implementing effective internal controls to safeguard all confidential personal information. As a result, MDIT has not identified any instances of lost or stolen personal information as a result of a security breach, for DELEG's AWARE system.

Regarding part a, MDIT and DELEG will work in conjunction with Department of Management & Budget (DMB) 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, MDIT and DELEG 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, MDIT, in conjunction with DELEG, will implement formal procedures to manage this process. To adequately secure customer data, the departments are utilizing encryption and secure transmission protocols to electronically provide customer data to third parties.

Regarding part c, DELEG's 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.

The expected date of compliance is December 31, 2009.

2. Change Control Process

MDIT and DELEG had not developed a comprehensive change control process for AWARE. Specifically:

- *a. MDIT and DELEG had not established documented change control policies and procedures.*
- *b. MDIT and DELEG did not use a standardized change request form.*
- *c. MDIT and DELEG did not maintain a complete log of production source code and data changes.*
- *d. MDIT did not establish effective controls to ensure the integrity of production source code versions.*

Agency Response: DELEG agrees with the finding.

MDIT has informed DELEG that it now has a comprehensive change management process and has developed formal procedures to include all change management processes. DELEG will comply with the MDIT comprehensive change control process, and will implement a similar internal system for the AWARE Support Unit.

The expected date of compliance is December 31, 2009.

3. Segregation of Duties

MDIT and DELEG did not segregate the duties of the database administrator by restricting the database administrator's access to the AWARE application and operating system.

Agency Response: DELEG agrees with the finding and has fully complied.

MDIT informed DELEG that upon notification of this finding; it immediately removed the database administrator's access to the operating system. Additionally, DELEG has removed administrator privileged access to the AWARE application.

4. Security Officer

DELEG had not established an information security officer position.

Agency Response: DELEG agrees and has complied.

DELEG recently assigned these responsibilities to the individual who also serves as its Internal Control Officer. The Security Officer will work with DELEG and MDIT management to establish department-wide standards and procedures to ensure the integrity and availability of information systems and data. Monitoring for compliance will be conducted both during DELEG's biennial evaluation process and on an ongoing basis.

5. Operating System Security Controls

DIT will respond to this finding.

6. Database Security Controls

MDIT and DELEG had not fully established security controls over the AWARE production, test, and reporting databases. Specifically:

a. *MDIT did not fully restrict certain users from having privileged access rights to 1 of the 3 databases.*
b. *a. MDIT did not fully restrict certain users from having privileged access rights to 1 of the 3 databases.*
c. *MDIT did not establish unique user accounts and passwords for all database users on 1 of the 3 databases.*
d. *MDIT did not use database audit logs to monitor database administrator activity on all 3 databases.*
e. *MDIT did not implement strong controls over database passwords on all 3 databases.*
f. *MDIT, in conjunction with DELEG, did not encrypt AWARE data on all 3 databases.*
g. *MDIT, in conjunction with DELEG, did not develop a complete data dictionary for the AWARE database.*

Agency Response: DELEG agrees with the finding.

MDIT has informed DELEG that it has initiated action to strengthen database security controls over the AWARE system. DELEG will provide assistance and support so that the timeframes MDIT has identified can be met.

Please refer to the DIT response to this finding for the expected date of full compliance.

7. Access Controls

DELEG had not established effective access controls over AWARE.

Agency Response: DELEG agrees and will comply.

DELEG will implement strong passwords, log-in audit logs, monitoring and stronger quarterly review of user access. In addition, DELEG has corrected user access rights; and DELEG staff (who are independent of the AWARE process) will perform semiannual reviews of access and related rights granted to MRS staff. DELEG has experienced some delays caused by various system and test server challenges.

The expected date of full compliance is October 31, 2009.

8. Data Processing Controls

DELEG did not implement data edits to ensure the integrity of AWARE data.

Agency Response: DELEG agrees and will comply.

DELEG will take actions to ensure that recurring payments exceeding $500 will be prohibited by data edits. Payments exceeding parameters have not occurred since November 2007 as a system put in place to immediately identify payments exceeding set parameters so that diagnosis can occur. Invalid service authorization dates and service date combinations last occurred in June 2008, prior to the code correction. DELEG has experienced implementation delays caused by various system and test server challenges.

The expected date of full compliance is October 31, 2009.

9. Data Matches

DELEG should match MRS customer data in AWARE to other data sources to determine the continued eligibility of customers.

Agency Response: DELEG agrees and will attempt to comply.

DELEG will consider matching customers to other data sources after assuring confidentiality of DELEG customer information and our ability to acquire agreements associated with data security and privacy controls with other data sources. Cost/benefit analysis factors and other logistical considerations will be assessed prior to deciding whether or not to implement this control.

The expected date of (conditional) compliance is April 30, 2010.

10. Audit Trails

DELEG did not fully develop and monitor audit trails for AWARE.

Agency Response: DELEG agrees and will comply.

The new version of AWARE (5.0) contains significant audit functionality. Working with MDIT Vantage Enterprise Group, we will implement this functionality incrementally.

The expected date of full compliance is October 31, 2009.