STATE OF MICHIGAN
DEPARTMENT OF INFORMATION TECHNOLOGY
LANSING

JENNIFER M. GRANHOLM
GOVERNOR

MICHIGAN DEPARTMENT OF
INFORMATION TECHNOLOGY
KENNETH D. THEIS
DIRECTOR

February 2, 2010

Mr. Doug Ringler, Director
Office of Internal Audit Services
State Budget Office
Romney Building, 6th Floor
111 S. Capitol Avenue
P.O. Box 30026
Lansing, Michigan 48909

Dear Mr. Ringler:

Enclosed is our final response to comments made in the Office of the Auditor General's Performance Audit of the General Controls over the Data Collection and Distribution System (DCDS) and the Human Resources Management Network (HRMN) of the Office of the State Budget, Civil Service Commission, and Michigan Department of Information Technology (MDIT) for the period October 1, 2007 through May 31, 2009.

MDIT is responding for all three findings which were directed at all departments. If you have any questions regarding this report, please feel free to call Ms. Fran Wresinski at (517) 243-1702.

Sincerely,

Signature Redacted

Tina Richardson, Internal Control Officer

Enclosure

c: Audit Distribution List
Phyllis Mellon
Lynn Draschil
Scott Thompson
Fran Wresinski

OAG AUDIT RESPONSE DISTRIBUTION LIST

Executive Office	Nathaniel Lake, Jr.
Office of the Auditor General	Scott Strong
Senate Fiscal Agency	Gary Olson
House Fiscal Agency	Mitchell E. Bean
Senate Appropriations Committee	Senator Ron Jelinek
House Appropriations Committee	Representative George Cushingberry, Jr.
Homeland Security and Emerging Technologies Committee	Senator Cameron Brown
Energy and Technology Committee	Representative Jeff Mayes
Office of Internal Audit Services	Rick Lowe
Office of the State Budget	Mike Moody
Civil Service Commission	Janet McClelland

AUDIT RESPONSE SUMMARY

Data Collection and Distribution System (DCDS) and
Human Resource Management Network (HRMN)
Office of State Budget
Civil Service Commission
Michigan Department of Information Technology
(October 1, 2007 through May 31, 2009)

I. Citations complied with:
1.b, 1.c, 1.d

II. Citations to be complied with:
1.a, 1.e – 1.h, 2.a – 2.f, 3.a – 3.e

III. Citations agency disagrees with:
None

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

1. Operating System Security and Access Controls

MDIT agrees with the audit recommendation to establish more effective operating system security and access controls. Three security and access control weaknesses have already been remediated, specifically weaknesses 1b, 1c, and 1d related to the operating systems' privileged account and start-up scripts.

Enforcement of strong password policy (item 1a) and security feature configuration (item 1e) will be implemented as part of host server refresh in order to reduce the risk of application side effects. In addition, the HRMN system will require changes to HRMN Security's user management application to allow for account resets by agency security administrators and to generate user passwords that comply with the new requirements. These items have been reviewed and requirements have been identified, but due to project prioritization and funding requirements, active remediation effort is not underway. The next steps include the definition of specifications and project plan for HRMN Security front end application changes. Funding for the server refresh project needs to be identified. MDIT will pursue this initiative depending upon cost assessments, project prioritization, potential benefits, levels of risk, and impact on its ability to support the State's business objectives within the current budget and resource constraints of the State.

Securing of sensitive operating system, application, and data files (item 1f) has been initiated. All identified files and directories must be reviewed individually making this a lengthy remediation process. A small percentage (approximately 10%) of these permissions has been corrected. MDIT will continue our analysis, review, and remediation process based upon level or risk, project priorities, and impact on its ability to support the State's business objectives within the current budget and resources constraints.

Logging and monitoring system administrator activities (item 1g) and security events (item 1h) have been partially remediated. MDIT Technical Services team has increased the amount of activity being captured in logs. However, improvements to the monitoring activities are still in progress. A project has been initiated to provide better logging and reporting capabilities across the State. Technical Services is currently building requirements for an RFP to purchase logging system software for this initiative. In addition, staffing for an independent quality assurance team has not been identified. MDIT will pursue this initiative depending upon cost assessments, potential benefits, levels of risk, and impact on its ability to support the State's business objectives within the current budget and resource constraints of the State.

2. **Database Security and Access Controls**

MDIT agrees with the audit recommendation regarding improvements to DCDS and HRMN database security and access controls. MDIT, in conjunction with OFM and CSC, is already working to implement solutions for some of the recommendations.

Development and implementation of policies and procedures for managing database security and access (item 2a) has been partially implemented. Various policies, procedures and guidelines have been developed and are being reviewed. Once approval has been received, these guidelines will be implemented. It is our intent to have the remaining policies, procedures and guidelines developed and ready for review by end of summer 2010. MDIT will continue this initiative depending upon cost assessments, potential benefits, levels of risk, and impact on its ability to support the State's business objectives within the current budget and resource constraints of the State.

Establishment of unique user accounts for HRMN and DCDS DBAs (item 2b) has been partially implemented. MDIT has created individual accounts for DBA's and has implemented access rights for supporting DBA's to eliminate the need for shared accounts. MDIT is currently in the final testing stage of these modifications. The next steps include developing usage procedures for primary and supporting DBA's and developing an incident escalation process. It is our intent to have the remaining procedures and processes implemented by the end of calendar year 2010. MDIT will continue this initiative depending upon cost assessments, potential benefits, levels of risk, and impact on its ability to support the State's business objectives within the current budget and resource constraints of the State.

Monitoring of HRMN and DCDS DBA and other privileged account activities (item 2c) has not been implemented due to resource contention between this initiative and project priorities. MDIT, in conjunction with OFM and CSC, will evaluate and remediate the security and access controls over the DCDS and HRMN databases depending upon the potential risks involved, potential solutions, and the availability of State resources.

Development of a strategy to detect and monitor security violations and unauthorized database activity (item 2d) has been initiated. The HRMN system is preparing to pilot logging modifications in the development region. However, no activity has occurred on DCDS due to resource contention between this initiative and project priorities. The next steps include completing testing on HRMN, implementing logging modifications on HRMN production, piloting and testing logging modifications on DCDS development, and implementing logging modifications on DCDS production. In addition, staffing for an independent quality assurance team has not been identified. It is our intent to have the logging modifications completed by end of summer 2010. MDIT will continue this initiative depending upon cost assessments, potential benefits, levels of risk, and

impact on its ability to support the State's business objectives within the current budget and resource constraints of the State.

Configuration of security settings such as password settings, profile settings, and configuration parameters for the HRMN and DCDS databases (item 2e) has been partially implemented. The profile settings and configuration parameters have been addressed for DCDS and HRMN. Password setting changes for HRMN are being tested. It is our intent to have the password setting changes for HRMN completed by end of summer 2010. Implementing the password setting changes for DCDS is a significant undertaking and will require its own project effort. MDIT, in conjunction with OFM and CSC, will evaluate this project depending upon the potential risks involved, potential solutions, and the availability of State resources.

Excessive access to the database management system granted by default to all database accounts (item 2f) has been partially remediated. This issue has been remediated on the HRMN databases, but has yet to be remediated on DCDS due to resource contention between this initiative and project priorities. MDIT, in conjunction with OFM and CSC, will evaluate this project depending upon the potential risks involved, potential solutions, and the availability of State resources.

3. **DCDS and HRMN Change Controls**

MDIT agrees with the audit recommendation to enhance the documentation procedures and documentation that exists within the DCDS and HRMN change control process. MDIT, in conjunction with OFM and CSC, is already working to implement solutions for some of the recommendations.

Development and implementation of formal enterprise change control policies and procedures (item 3a) has been initiated. MDIT has revised Technical Standard 1370.01 and several other procedures. These procedures are scheduled to be presented to the MDIT Cross Functional Review Team in January, 2010. The Enterprise Change Governance Board is addressing formal enterprise change control policies and procedures. MDIT will continue this initiative depending upon cost assessments, potential benefits, levels of risk, and impact on its ability to support the State's business objectives within the current budget and resource constraints of the State.

Categorization of changes by type and significance in the enterprise change control process (item 3b) has been initiated. The Enterprise Change Governance Board is actively working on a model to categorize changes by type and significance. It is our intent to have this implemented by June, 2010. MDIT will continue this initiative depending upon cost assessments, potential benefits, levels of risk, and impact on its ability to support the State's business objectives within the current budget and resource constraints of the State.

Improvement of the assessment of security and risk analysis information associated with each change (item 3c) has been initiated. MDIT Agency Services attempts to obtain details from the change owner in order to provide the business clients information for their change management and testing process. MDIT will continue efforts to improve this process depending upon cost assessments, potential benefits, levels of risk, and impact on its ability to support the State's business objectives within the current budget and resource constraints of the State.

Performing integrated testing of operating system changes prior to implementation in the production environment (item 3d) has not been implemented due to resource contention between this initiative and project priorities. Increased communications between Technical Services and Agency Services of changes and change impacts needs to be implemented. MDIT, in conjunction with OFM and CSC, will evaluate and remediate the change controls over the DCDS and HRMN systems depending upon the potential risks involved, potential solutions, and the availability of State resources.

Establishment of controls to monitor the effectiveness of MDIT's change control process (item 3e) has not been implemented due to resource contention between this initiative and project priorities. Technical Services is currently building requirements for an RFP to improve the effectiveness of MDIT's change control process. MDIT will pursue this initiative depending upon cost assessments, potential benefits, levels of risk, and impact on its ability to support the State's business objectives within the current budget and resource constraints of the State.