JENNIFER M. GRANHOLM
GOVERNOR

STATE OF MICHIGAN
DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
LANSING

KENNETH D. THEIS
DIRECTOR

April 19, 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 Unisys Mainframe, Michigan Department of Information Technology (MDIT) for the period October 1, 2008 through August 31, 2009.

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
Dan Lohrmann
Carol Sherman
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

AUDIT RESPONSE SUMMARY

I. Citations complied with:
2b

II. Citations to be complied with:
1a – 1e, 2a, 3a - 3d, 4a - 4b, 5a – 5d

III. Citations agency disagrees with:
None

Performance Audit of
Unisys Mainframe General Controls
Agency Response

1. **Mainframe Access Controls**
MDIT agrees with the audit recommendation to establish more sufficient controls over the Unisys mainframe computers. We have collected all the required information to implement the corrective action associated with finding 1a and are in the process of identifying the high risk access rights. We are currently working on the information needed to have a meeting with the department security administrators related to corrective actions required to remediate findings 1b and 1c since these deal with the department security, not MDIT security. The analysis of the access rights review process will be completed by May 14th, 2010. We are currently working on the form required to implement corrective action associated with finding 1d. We have finished reviewing our current settings and process to help us evaluate what needs to be done to resolve finding 1e. We can implement some requirements for strong passwords, but other requirements will be researched and tested this summer.

2. **Mainframe File Security**
MDIT agrees with the audit recommendation to establish more effective security controls over the Unisys mainframe computer files. We have completed the major first step in remediating finding 2a. Spreadsheets of every single file on the Unisys MCP system with their security attributes have been provided to the owning departments' Security Administrators. To complete 2a the Department Security Administrators must review the spreadsheets we provided and make the necessary changes to their files security settings. Remediation related to finding 2b has been completed.

3. **BL/Source and BL/Sched Software Access Controls**
MDIT agrees with the audit recommendation to more effectively manage and monitor the use of BL/Source and BLSched software products. In relation to corrective action associated with finding 3a, we are creating a report by 3rd party softwareproduct of privileged users (high risk). This will be completed by April, 2010. We are in the process of developing an information check sheet and forms to implement the corrective action associated with finding 3b. A meeting will be scheduled with the Department Security Administrators to outline actions required. In regards to finding 3c, we have identified the current password composition and are working with the vendor. We should have a response by April, 2010. We are identifying current policy documents needed to implement corrective action associated with finding 3d.

4. **Physical and Environmental Controls**

MDIT agrees with the audit recommendation to establish more effective access controls to the computer facilities that house the Unisys mainframe computer. We have created a draft policy that will be submitted to the Enterprise Cross-Functional Policy Review Team for their review and approval in April, 2010 which will comply with finding 4a. We now receive a feed from HRMN for every pay period that provides a list and full HRMN information every quarter. Reports still need to be generated. We are looking to complete this by June, 2010 to implement the corrective action required for finding 4b.

5. **Backup and Disaster Recovery Controls**

MDIT agrees with the audit recommendation to establish more sufficient backup and disaster recovery processes. Regarding the corrective action required to comply with finding 5a, agencies can already run the Recovery history report in BL/Sched. We are obtaining information on how to put this information in Strohl. Processes are currently being developed for the operating system. Test and final documentation of this process will be completed during the yearly Disaster Recovery Test. Procedures are already in place to document the Disaster Recovery process to comply with finding 5b. A process to publish the results will be added and tested in this years Disaster Recovery testing. A meeting will be held with management to determine how the approval process should work to implement the corrective action associated with finding 5c. This will be completed by May, 2010. Remediation required to comply with finding 5d has not been started yet, but will be started within the next two months.