STATE OF MICHIGAN

RICK SNYDER
GOVERNOR

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
LANSING

JOHN E. NIXON, CPA
DIRECTOR

July 23, 2012

Doug Ringler, Director
Office of Internal Audit Services
Office of the State Budget
George W. Romney Building
111 South Capitol, 6th Floor
Lansing, Michigan 48913

Dear Mr. Ringler:

In accordance with the State of Michigan, Financial Management Guide, Part VII, attached is a summary table identifying our responses and corrective action plans to address recommendations contained within the Office of the Auditor General's audit report of the Michigan Administrative Information Network (MAIN) Security, State Budget Office and the Department of Technology, Management & Budget.

Questions regarding the attached summary table or corrective action plans should be directed to me.

Sincerely,

Signature Redacted

Michael R. Gilliland, Director
Financial Services

Attachment

c: Rep. Chuck Moss, Chair, House Appropriations
Senator Rodger Kahn, Chair, Senate Appropriations
Melissa Schuiling, Office of the Auditor General
Dennis Muchmore, Executive Office
Dick Posthumus, Executive Office
House Fiscal Agency
Senate Fiscal Agency
David Behen, DTMB
Rick Lowe, DTMB
Kurt Weiss, DTMB
Matt Sweeney, DTMB
Lynn Draschil, DTMB
Scott Thompson, DTMB
Nancy Duncan, SBO
Mike Moody, SBO

Performance Audit
Michigan Administrative Information Network
(MAIN) Security
State Budget Office and
Department of Technology, Management and Budget
Audit Report Issued: October 2010

Summary of Agency Responses to Recommendations

1. Audit recommendations DTMB fully complied with:

2. Audit recommendations DTMB agrees with and will comply:

3. Audit recommendations DTMB disagrees with:

4. Audit recommendations DTMB neither agrees nor disagrees with: Finding #1, #2, #3, #4, #5, #6.

Recommendation 1 – Monitoring Controls:
The Department of Technology, Management & Budget (DTMB) had not established, and did not ensure that the TPSO established, effective controls to monitor system activity and identify security violations.

Agency Response:
A work group was created in FY 2011 to consider responses to these audit findings. The group consists of representatives from DTMB-IT Agency Services, the TPSO (IBM), DTMB-Office of Enterprise Security, and State Budget Office-Office of Internal Audit Services. The work group meets weekly and is tasked with developing recommended corrective actions for review and approval by the State Budget Office-Office of Financial Management. DTMB and the TPSO are continuing to research cost effective improvements. As a result, the department does not have an estimated time of completion.

Recommendation 2 – Mainframe Security Function:
DTMB had not implemented all components of an effective mainframe security function.

Agency Response:
DTMB-IT filled two Security Officer positions in fiscal year 2010- 2011 and is continuing to isolate and pursue the appropriate access to the appropriate resources where ever possible. The Security Officer role provides a separation between the existing Security Administrator duties from duties of the DTMB-IT Development Manager (Part B).

The training and responsibilities of these Officers (Parts A and C) are being developed over time, with full implementation expected during 2012.

Weaknesses noted in part D of the finding (AUDITOR privileges on the mainframe) were fully remediated in 2011.

Recommendation 3: Security Requirements
DTMB did not ensure the completeness and effectiveness of security requirements defined in the GSD-331.

Agency Response:
In Sept 2011, DTMB-IT and the TPSO, in cooperation with OES, Attorney General and OFM, strengthened the security banner on all MAIN login pages in all environments (Part B.4).

The work group and OFM are working towards new password rules to strengthen password composition, aging and history (Part B.1). .

Cleanup has been performed on inactive user accounts. Policies and procedures are being developed to provide guidance for account maintenance, review, and accountability, helping to ensure that inactive accounts are properly revoked from the system in a timely manner (Part B.2). SBO-OFM will provide review and approval for all policies and procedures.

DTMB is working to act on the identified weaknesses to better comply with GSD-331. DTMB-IT and the TPSO have drafted changes to the GSD331, to document deviations from TPSO security recommendations (Part C). These will be considered during the next review of the document.

All other parts of this finding (Findings A, B.3) will be addressed during the GSD-331 refresh negotiations in calendar year 2012. These negotiations will also consider information provided by the new hosting contract and the findings reported in this audit. The department does not have an estimated time of completion.

Recommendation 4: Risk Assessments
OFM and DTMB had not completed risk assessments of MAIN general and application controls and of the risks associated with using a TPSO.

Agency Response:
While a formal Risk Assessment has not yet been performed, an informal review of risks was done in conjunction with the negotiations for the new Hosting Contract. IBM's response to the RFP provided documentation of the physical security of their Data Center. DTMB, including the Office of Enterprise Security, reviewed and accepted this contractor's data center security posture as satisfying the needs of a Tier 3 Data Center, as required for MAIN/FACS. The hosting contract includes provisions so that continued risk and vulnerability assessments are performed by the TPSO (IBM) of their hosting center facilities and services. DTMB and SBO-OFM will develop a periodic review process of the physical security requirements from the SAS-70 review, as part of the resolution for finding 5 (see below).

As part of the recently awarded MAIN hosting contract, several security measures have been agreed to and will be implemented in 2012, to ensure the confidentiality of MAIN/FACS data, including the implementation of encryption for data at rest, data on off-site tape, and data in transmission between the Boulder data center and the State of Michigan hosting centers. The hosting contract has produced updated documentation for encrypting data in route. In addition, as part of the new contract, DTMB and IBM are preparing to roll-out a new end-user terminal emulation package which will provide encryption between the Boulder data center and each individual user end-point. The department does not have an estimated time of completion.

Recommendation 5: Effectiveness of the TPSO's Controls
OFM and DTMB did not fully implement the controls identified in the User Control Considerations section of the TPSO's Statement on Auditing Standards No. 70 report (SAS 70 report*). In addition, OFM and DTMB did not document their assessment of internal control exceptions identified in the TPSO's SAS 70 report.

Agency Response:
Corrective action for this recommendation is being coordinated with DTMB efforts in response to Finding 4. IBM is providing information regarding a hosting center risk and security assessment as part of the negotiations for the new Hosting Contract and the upcoming refresh of the GSD-331 document.

IBM, as the TPSO for multiple organizations besides the State of Michigan/MAIN-FACS, has a SAS-70 evaluation done for a select subset of its clients, not necessarily including the State of Michigan/MAIN-FACS. Due to the sensitive nature of a SAS-70 report, IBM is able to provide only a high-level summary of the report to the State of Michigan for review. DTMB, along with the Office of Enterprise Security, will work to create a methodology to confirm IBM's controls and the effectiveness of those controls as described in the summary. DTMB and OFM will work to ensure that controls are in place (policies and procedures) as recommended by the SAS-70 report. This work is expected to be completed in 2012.

Recommendation 6: Access to Resources
OFM and DTMB had not established effective access controls over MAIN operating system, application, and data resources.

Agency Response:
Privileged access rights were reviewed and corrective actions were taken to revoke privileges that were no longer appropriate (Part A). Access rights to system files and resources were reviewed and corrective actions were taken to revoke access rights that were no longer appropriate (Part B). Access rights to production application data sets were reviewed and corrective actions were taken to revoke/modify inappropriate access rights (Part C). Access rights to databases were reviewed and corrective actions were taken to revoke/modify inappropriate access rights (Part D).

Policies and Procedures are under development to provide effective access controls over MAIN operating system and data resources (covers all parts of this Finding), including individual access privileges as documented in Parts A, B, C and D. These will provide processes to monitor, manage and perform regular reviews for compliance. The SBO-OFM review/approval phase for these policies is expected to begin late 2011.

Response for Parts E, F and G will be included in the new set of policies and procedures to be reviewed and approved by SBO-OFM.

Changes to the access privileges for the scheduling software (Part A.5) has extensive ramifications to system operations and would require substantial time and expense for a redesign effort. The scheduling software does provide role-based access controls, so DTMB will work with the TPSO to ensure that secondary controls such as compliance monitoring are in place as resolution for this finding. TSIEM had been proposed as a possible monitoring tool for these privileged activities, but with the rejection of that proposal, DTMB-IT will continue researching alternative cost effective solutions. As a result, the department does not have an estimated time of completion.