72 (Rev. 04-15)

STATE OF MICHIGAN
DEPARTMENT OF TREASURY
LANSING

RICK SNYDER
GOVERNOR

NICK A. KHOURI
STATE TREASURER

August 15, 2016

Bryan Weiler, Acting Director
Office of Internal Audit Services
Office of the State Budget
George W. Romney Building
111 South Capitol, 6th Floor
Lansing, MI 48913

Dear Mr. Weiler,

In accordance with the State of Michigan, Financial Management Guide, Part VII, the following is a summary identifying our response and corrective action plan to address recommendations contained within the Office of the Auditor General's Performance Audit of the Investment Related Systems, Bureau of Investments (BOI), Department of Treasury and Department of Technology, Management, and Budget (DTMB), Report Number 271-0585-15, from October 1, 2013 – September 30, 2015.

1. Audit recommendations the agency agrees with and will comply:

Q2 Application Security and Access Controls:

We recommend that the BOI, in conjunction with DTMB, fully establish and implement security and access controls to properly protect the Q2 application and data.

Agency Plan:

BOI believes there is a low risk of unauthorized or inappropriate access to the Q2 application, which does not maintain any personal, tax, or exempt information. In addition, multi-factor security access controls are in place.

Going forward, the BOI, in conjunction with DTMB, will comply as follows:

a. Document the authorization of Q2 user access rights every 120 days to ensure that user access rights remain appropriate. As evidence of the compliance, all applicable documentation will be reviewed, printed, signed, and dated. BOI staff completed the latest review in May 2016. A procedure for this process will be completed by September 2016, barring any unforeseen issues.
b. Monitor the appropriateness of user activity by reviewing Q2 logs. Also, other internal controls are in place to detect inappropriate activity, such as reconciliation with third party data. BOI staff is working with the vendor to establish a process that can document the review of the Q2 logs. It is anticipated

that it will be completed by August 2016, barring any unforeseen issues. A procedure for this process will be completed by November 2016, barring any unforeseen issues.

c. Review user access rights every 120 days to ensure that rights remain appropriate. As evidence of the review, all applicable documentation will be printed, signed, and dated. BOI staff completed the latest review in May 2016. A procedure for this process will be completed by September 2016, barring any unforeseen issues.

d. Review and update the Q2 security plan. The agencies are working with the vendor for the Q2 application to complete a security plan (i.e., the DTMB-170), which after completion, the security plan will be reviewed per Treasury Policy, Security Plan ET-03183, every three years or sooner if there is a significant change to the system. It is anticipated that the security plan for the upgraded Q2 system will be completed by September 2016, barring any unforeseen issues. A procedure for this process will be completed by November 2016, barring any unforeseen issues.

Q2 Database Security Configurations and User Access Controls:

We recommend that DTMB, in conjunction with BOI, fully establish and implement security and access controls over the Q2 database.

Agency Plan:

The Q2 application was recently upgraded to a newer system that resolved many of the noted issues. For the issues still needing attention, DTMB and BOI are working with the vendor to comply as follows:

a. Ensure the effective configuration of the Q2 database security settings, such as profile settings, implementing security patches and configuration parameters. The security settings for the Q2 database shall be in compliance with best practices commensurate with the upgrade of the Q2 software and in accordance with the architecture of the QED platform. However, there are a few instances where the database file system permissions could not be changed as it would result in database malfunction. Vendor completed all software compatible changes with the implementation in May 2016.

b. Sufficiently restrict access to the Q2 database. The upgrade to the current version of the Q2 software provided as a service includes a managed MySQL version in which blank passwords and anonymous accounts are programmatically prohibited as an installation, configuration, and provisioning best practice. Furthermore, to the greatest extent possible, the Q2 software has been configured in accordance with BOI and DTMB requirements to include named MySQL maintenance accounts for QED staff. Vendor completed all software compatible changes with the implementation in May 2016.

c. Document and maintain the authorization and approval of user access to the Q2 database. Consistent with State of Michigan policies as applicable to DTMB and BOI, the agencies will create a Service Level Agreement (SLA) with the vendor in order to define the requirements for the Q2 software provided as a service, including standard operating procedures for the definition and maintenance of

authorized/approved QED and client staff user accounts. It is anticipated that the SLA will be completed by December 2016, barring any unforeseen issues. A procedure for this process will be completed by September 2016, barring any unforeseen issues.

d. Use database audit logs to monitor the activity of database administrators and other privileged accounts. The upgrade to the current version of the Q2 software provided as a service includes a managed MySQL version in which Enterprise Audit Logging features are programmatically enabled during installation, configuration, and provisioning. BOI has requested that the vendor supply MySQL database logs for review by BOI and DTMB. Upon receipt of the logs, a formal review will be completed every 120 days. We anticipate that the process will begin October 2016, barring any unforeseen issues. A procedure for this process will be completed by October 2016, barring any unforeseen issues.

2. Audit recommendations the agency complied with:

Bloomberg AIM Access Controls:

We recommend that BOI fully implement access controls to ensure the authorization of Bloomberg AIM users.

Agency Plan:

To address the access control issues with Bloomberg AIM, the BOI has completed the following:

a. Documented authorization of user access to Bloomberg AIM, with the creation of a Bloomberg AIM New User/Change Request Form, for use with all future users of the system. BOI and DTMB staff developed the Bloomberg AIM New User/Change Request Form in February 2016. BOI staff completed the latest review in May 2016. A procedure for this process was completed in March 2016.

b. Documented the review of user activity and account management logs, which are electronically signed, dated, and stored outside the system. BOI staff started the daily review in January 2016, with evidence of the signed documentation being as of March 2016. A procedure for this process was completed in July 2016.

c. Review user access rights every 120 days to ensure that rights remain appropriate. As evidence of the review, all applicable documentation are printed, signed, and dated. BOI staff completed the latest review in May 2016. A procedure for this process will be completed by September 2016, barring any unforeseen issues.

3. Audit recommendations the agency disagrees with: None

Should you have any questions regarding the summary of our corrective action plan, please contact Robert L. Brackenbury at (517) 373-3142 or at BrackenburyR@michigan.gov.

Sincerely,

Signature Redacted

Jon M. Braeutigam
Senior Chief Investment Officer
Deputy State Treasurer
Bureau of Investments

cc: Jarrod Agen, Executive Office
Wendy Wisniewski, Executive Office
Doug Ringler, Office of the Auditor General
Mary Ann Cleary, House Fiscal Agency
Ellen Jeffries, Senate Fiscal Agency
Laura Cox, House Appropriations Sub-committee
Jim Stamas, Senate Appropriations Sub-committee
Jeff Farrington, House Standing Committee
Jack Brandenburg, Senate Standing Committee
Nick Khouri, Treasury
Joe Fielek, Treasury
Rick Lowe, Office of Internal Audit Services
Bruce Hanses, Treasury
Robert L. Brackenbury, Treasury
John Juarez, DTMB