STATE OF MICHIGAN

RICK SNYDER
GOVERNOR

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
LANSING

JOHN E. NIXON, CPA
DIRECTOR

December 2, 2013

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 Data Exchange Gateway, Department of Technology, Management & Budget.

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

Sincerely,

Signature Redacted

Mike Gilliland, Director
Financial Services

cc: Rep. Joseph Haveman, Chair, House Appropriations
Sen. Roger 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
Lynn Draschil, DTMB
Dan Lohrmann, DTMB
Judy Odett, DTMB
Kurt Weiss, DTMB
John Juarez, DTMB
Richard Novello, DTMB
Richard Reasner, DTMB
Vern Klassen, DTMB
Rick Lowe, DTMB
Chris Harkins, DTMB

Performance Audit of the Data Exchange Gateway (071-0592-13)
Department of Technology, Management and Budget

Audit Period: October 1, 20122 through June 30, 2013

Summary of Agency Responses to Recommendations

1. Audit recommendations DTMB fully complied with: None
2. Audit recommendations DTMB agrees with and will comply: Finding # 1, 2, 3, 4, 5
3. Audit recommendations DTMB disagrees with: None

Agency's plan to address the recommendations:

1. Secure Electronic Transfers

DTMB agrees with the recommendation and has established the following remediation activities:

a.) Technical Standard 1340.00.11, which was implemented and published on June 5, 2013, established the standard for electronic file transfers. In addition, DTMB Cyber Security will utilize Data Loss Prevention (DLP) tools, once procured, to monitor unsecure FTP traffic. Existing tools will be utilized until the procured tools are implemented.

b.) DTMB's unified approach to information technology management for the DEG includes the generation and publication of a data classification standard and procedure in compliance with State of Michigan (SoM) policy 1340 - Information Technology, Information Security Policy which requires data owners to:

a. Ensure data management is in compliance with Federal and State laws and SoM policies and procedures.

b. Ensure agency information is identified and classified based on sensitivity, criticality and risk.

c. Ensure information security controls are applied in a manner consistent with the value of the information.

d. Ensure a review process in place for on-going compliance.

The data classification standard, with an expected implementation by December 31, 2014, will require the data owner to attest to regulatory compliance. DTMB, in compliance with said policy, will advise and implement Agency prescribed controls and safeguards. As of June 5, 2013, all file transfers not utilizing the DEG must now request an exception in compliance with standard 1305.00.02 - Technical Policy and Product Exception, where exception requests are reviewed, and all actions, deliberations and results will be documented. In addition, all current non-DEG exceptions will be reviewed and a compliance date will be determined. Electronic File Transfer Technical Standard 1340.00.11 will be updated by June 30, 2014 and include a grandfather clause, with the aforementioned compliance to be within one year of the approved update.

c.) DTMB will develop a communication plan by March 31, 2014 to inform agencies of the newly published standard, the benefits of using the DEG and the proper procedures to utilize the system. DTMB has also implemented an annual review of the file transfer

procedures. DTMB believes increased awareness and education will promote usage of the platform and reduce transfer costs for all clients.

DTMB anticipates overall compliance by December 31, 2014.

2. Infrastructure of the DEG

DTMB agrees with the recommendation and has established the following remediation activities:

a.) DTMB will perform a hardware/software migration of the DEG platform by March 31, 2014. Virus scanning will be implemented as part of that new solution, which will prevent threats from entering and/or spreading on the State's network.

b.) DTMB has developed a Service Catalog for the DEG service which includes terms of use and service levels. The catalog will be reviewed annually by management to ensure continued accuracy and relevance.

c.) DTMB will perform a hardware/software migration of the DEG platform by March 31, 2014. Subsequent to the migration, DTMB will have the ability to restrict the use of unsecured FTP and will establish an exception process for data that has been certified as non-sensitive according to established policies. Related to the DEG hardware/software migration – The Enterprise Architecture Solution Assessment (EASA), Infrastructure Solution Request (ISR), and Hosting documents have all been approved. The new 7 Virtual Machine (VM) servers are setup and ready for application software load and configuration. The Discovery Statement of Work (SOW) with the vendor (Ipswitch) is on target.

3. Operating System Security and Access Controls

DTMB agrees with the recommendation and has established the following remediation activities:

DTMB is in the process of implementing the Lightweight Directory Access Protocol (LDAP) for enterprise wide, system level identity management. LDAP integration will provide additional controls and improve granular access to satisfy access requirements. The expected implementation date is September 30, 2014. It is important to note that global data at rest encryption was implemented in May 2013. Additionally, DTMB is transitioning to an automated configuration management tool which will assist to rapidly deploy, maintain, and audit internal controls. In addition, the tool will prevent changes from required minimal service configurations and deviations from approved build procedures. The implementation date is July 31, 2014.

4. Database Management System Security and Access Controls

DTMB agrees with the recommendation and has established the following remediation activities:

a.) DTMB will create internal procedures by June 30, 2014, to document the hardening process for the DEG database, as defined by best practices from the Center for Internet Security.

b.) DTMB will establish effective security and access controls over the DEG database by June 30, 2014, as defined by best practices from the Center for Internet Security.

5. Access Controls Over the DEG

DTMB agrees with the recommendation and has established the following remediation activities:

DTMB will perform a hardware/software migration of the DEG platform by March 31, 2014. The migration will position DTMB to implement effective authentication security controls for the system and comply with DTMB Technical Standard 1335.00.03 - Identification, Authentication and Access Control. However, DTMB anticipates significant challenges related to mandating password expirations for some external trading partners. Regarding the DEG hardware/software migration, the Enterprise Architecture Solution Assessment (EASA), Infrastructure Solution Request (ISR), and Hosting documents have all been approved. The new 7 Virtual Machine (VM) servers are setup and ready for application software load and configuration. The Discovery Statement of Work (SOW) with the vendor (Ipswitch) is on schedule to meet its deadline.