72 (Rev. 01-19)

STATE OF MICHIGAN
DEPARTMENT OF TREASURY
LANSING

GRETCHEN WHITMER
GOVERNOR

RACHAEL EUBANKS
STATE TREASURER

June 4, 2020

Rick Lowe, 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. Lowe,

In accordance with the State of Michigan, Financial Management Guide, Part VII, the following is our corrective action plan to address recommendations contained within the Office of the Auditor General's Performance Audit of the Michigan Integrated Tax Administration System (MIITAS), Report Number 271-0595-19, from June 1, 2018 – September 30, 2019.

1. Audit recommendations the agency complied with:

Finding #5 – Improvements Needed in Tax Refund Interface Controls:
We recommend that Treasury improve its interface controls to ensure that tax refund checks are sent to the taxpayer address indicated on the return.

Agency Plan:
Undeliverable refunds are returned to Treasury to be reviewed and processed. In January 2020, processes were implemented to allow address updates prior to sending the refund.

Finding #6 – Change Management Process Improvements Needed:
We recommend that Treasury, in conjunction with DTMB, fully implement effective change controls over MIITAS to ensure that system changes are authorized and operating as intended before implementation.

Agency Plan:
In June 2019, Test Plans were fully implemented for maintenance and operations change activity. A Technical Review Board was convened to perform structured walkthroughs. Beginning in January 2020, DTMB implemented full separation of duties for maintenance and operations activities by executing System Integration Testing (SIT) in advance of Treasury User Acceptance Testing (UAT). Positive and negative test result evidence have been maintained since January 2020.

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

Finding #1 - Monitoring of Security-related Events Needed:
We recommend that Treasury, in conjunction with DTMB, monitor security-related events within MIITAS to help facilitate the ongoing awareness of threats, vulnerabilities, and information security.

Agency Plan:
Treasury and DTMB were aware of this weakness and initiated a project in 2018 to select and implement a Governance, Risk and Compliance (GRC) tool. The GRC tool was successfully implemented and deployed in September 2019 and along with the improved business processes, provides the capability to monitor security-related events within MIITAS. Treasury and DTMB continue to develop and implement procedures to facilitate the ongoing awareness of threats, vulnerabilities and information security. A feasibility study will be conducted and completed by July 1, 2020 to determine which procedures will be supported by available resources.

Finding #2 - Effective Access Controls Not Established and Implemented:
We recommend that Treasury fully establish and implement effective access controls over MIITAS to help ensure that data is secure and system controls are operating as intended.

Agency Plan:
Treasury was aware of weaknesses with access control processes and initiated a project in 2018 to select and implement a Governance, Risk and Compliance (GRC) tool. The GRC tool was successfully implemented and deployed in September 2019 and along with the improved business processes, have mitigated and reduced these weaknesses. Treasury continues to refine its use of the GRC tool to enforce least privileged access and to better monitor access within the system.

A. Treasury did not sufficiently restrict high-risk access within MIITAS in accordance with Treasury policy ET-03179.

   GRC requires justification for the needed access as well as requiring approvals from the appropriate business owner as well the security administrator before allowing a user to have access. GRC also allows Treasury to set an end date for temporary access, which limits the risk of access no longer being needed.

   The emergency access management module of GRC has been implemented and high-risk transaction codes identified by Treasury are being moved into roles that are used on a limited basis. This process is expected to be completed by June 2020.

   Additionally, Treasury is completing a segregation of duties risk analysis leveraging the SAP GRC tool which will allow Treasury to better limit and remove access which is considered to be high-risk. The risk analysis is expected to be completed by July 2020.

B. Treasury did not fully implement effective controls over non-user accounts.

Treasury has reviewed the non-user accounts that were questioned during the audit and locked all non-user accounts where feasible. Treasury is currently reviewing other non-user accounts that are currently being used in MiITAS and determining the appropriate access. This process requires more extensive testing as removing access from the non-user accounts may cause inadvertent issues within MiITAS including system outages. A plan for restricting access for these non-user accounts will be developed and implementation will begin by the end of June 2020.

C. Treasury should improve its periodic access review process.

GRC significantly reduced the manual work that was previously required to remove access from multiple environments. Treasury also increased their MiITAS monitoring staff to reduce the risk that user access is not removed timely. We consider this part of the finding to be complied with.

D. Treasury should improve its segregation of duties over incompatible job functions.

Treasury is completing a segregation of duties risk analysis leveraging the SAP GRC tool which will automatically alert security administrators of MiITAS users with incompatible roles. The risk analysis is expected to be completed by July 2020.

E. Treasury should improve its documentation of user access.

Treasury continues to train security liaisons about adequate supporting rationale for requesting access to MiITAS. Additionally, GRC requires the necessary approvals prior to allowing access to MiITAS which replaces the previous manual process. We consider this part of the finding to be complied with.

Finding #3 – Improvements Needed Over Configuration Management Controls:
We recommend that DTMB, in conjunction with Treasury, fully establish and implement effective configuration management controls to ensure that MIITAS is protected from threats and vulnerabilities.

Agency Plan:
DTMB identified gaps in the configuration management process and addressed these gaps. In January 2020, DTMB completed implementation of new configuration management tools. DTMB continues to develop documentation and operationalize internal procedures to establish configuration management processes specific to SAP. The internal procedures will be documented by October 30, 2020.

Finding #4 – Vulnerability Management Process Improvements Needed:
We recommend that DTMB improve it MIITAS vulnerability management process to ensure that threats are identified and remediated to reduce the risk of exploitation.

Agency Plan:
In April 2020, DTMB approved a plan to initiate a monthly patching cadence for SAP Systems. Patching began in May 2020 in the Sandbox environment and will continue to Production environments in June 2020. It is anticipated that all vulnerabilities identified during the OAG audit will be remediated by August 2020 in accordance with the monthly patching cadence.

3. Audit recommendations the agency disagrees with: None

Should you have any questions regarding the corrective action plan, please contact Dave Mefford at: 517-636-5546 or at: MeffordD@michigan.gov

Sincerely,

Signature Redacted

Sally Durfee
Chief of Staff
Department of Treasury

Signature Redacted

Andrey Verevko
General Manager, Agency Services
Department of Technology, Management And Budget

Cc: JoAnne Huls, Executive Office
Jay Rising, Executive Office
Doug Ringler, Office of the Auditor General
Mark Huizenga, House Appropriations Sub-committee
Jim Stamas, Senate Appropriations Sub-committee
Jason Sheppard, House Standing Committee
Mike Shirkey, Senate Standing Committee
Mary Ann Cleary, House Fiscal Agency
Christopher Harkins, Senate Fiscal Agency
Rachael Eubanks, Treasury
Ann Good, Treasury
Glenn White, Treasury
Dave Mefford, Treasury
Ryan McElhone, Treasury
Richard Znidarsic, Treasury
Susan Nichols, Treasury
Scott Lonberger, Treasury
Ken Osborne, Treasury
Danelle Gittus, Treasury

Ron Leix, Treasury
Stacey Bliesener, Treasury
Bruce Hanses, Treasury
Lucy Pline, DTMB
Cassandra Huguelet, DTMB
Patricia Chooi, DTMB
Mike Williams, DTMB OIAS
Fran Thelen, DTMB OIAS