STATE OF MICHIGAN

GRETCHEN WHITMER
GOVERNOR

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
LANSING

BROM STIBITZ
ACTING DIRECTOR

September 18, 2020

Mr. Richard Lowe, Chief Internal Auditor
Office of Internal Audit Services
Office of State Budget
George W. Romney Building
111 South Capitol, 6th Floor
Lansing, Michigan 48933

Dear Mr. Lowe:

In accordance with the State of Michigan, Financial Management Guide, Part VII, as initially submitted on 2/25/2020, following is a summary table identifying our ongoing responses and corrective action plans to address recommendations contained within the Office of the Auditor General's audit report of MILogin.

If you have any questions, or if we can be of further assistance, please don't hesitate to contact me directly.

Sincerely,

Signature Redacted

Brom Stibitz
Acting Director (Chief Deputy Director)
& Chief Information Officer
DTMB

Attachment: DTMB Corrective Action Plan Response to OAG MILogin Audit (071-0570-18)

CC: Senator Edward McBroom, Senate Oversight Committee
Representative Matt Hall, House Oversight Committee
Senator Roger Victory, Chair, Senate Appropriations Subcommittee on General Government
Representative Mark Huizenga, Chair, House Appropriations Subcommittee on General Government
Zack Kolodin, Executive Office of the Governor
Doug Ringler, Auditor General
Laura Clark, Acting Chief Security Officer
Jack Harris, Chief Technology Officer

Cindy Peruchietti, Director Agency Services
Eric Swanson, Director Center for Shared Solutions
Rex Menold, Acting Director of Enterprise Information, Content and Identity Management
Michelle Lange, Chief of Staff

DTMB
CSS MILogin
Summary of Agency Responses to Recommendations

1. Audit recommendations DTMB remediated: #2
2. Audit recommendations DTMB at least partially agrees with and will continue to remediate the parts DTMB agrees with: #1, #3, #4
3. Audit recommendations DTMB fully disagreed with: None

Agency Responses to Recommendations

Finding #1 – Improved Account Management and Monitoring needed

DTMB partially agreed with the recommendation.

MILogin is a gateway to State Agency applications for individuals or businesses doing business with or on behalf of the State of Michigan and State workers. MILogin does not grant access to Agency applications or Agency application data. Only State Agencies have the ability to grant access to Agency applications and Agency data.

Regarding part a. of the finding, DTMB agrees that it has not fully established processes to monitor privileged MILogin user activity such as the specific activities identified within the OAG's audit report. Implementing additional processes to expand DTMB's monitoring of privileged MILogin user activities will require additional resources, including funding and tools. DTMB will consider the OAG's recommendation in future budget cycles. DTMB has, however, implemented processes to mitigate related risks, to include:

- Forensic analysis tools to assist in monitoring MILogin.
- SOM Windows Network Accounts must use multi-factor if accessing the SOM network remotely.
- SOM Windows Network Accounts must use Multi-Factor Authentication to log-in to Office 365 services.
- State managed devices are managed for possible bot infections.
- Suspicious windows account sign-in activity is monitored.
- Impossible Travel for Windows accounts is monitored.
- Use of data loss prevention monitoring tools.
- E-mail message size is limited.
- Access to Internet Personal Storage services is limited.

Regarding part b. of the finding, DTMB agreed with the need to utilize unique administrative accounts for all administrative work. As of December 2019, DTMB now utilizes unique administrative accounts for all administrative work.

Regarding part c. of this finding, DTMB partially agrees that it has not fully established controls over accounts utilized in the MILogin production environment.

DTMB does not agree the MILogin administrator accounts cited in the OAG's audit report are test accounts; the accounts are verification accounts used by DTMB to perform validation of MILogin functionality and perform daily health checks, in accordance with SOM Technical Standard 1340.00.060.04. DTMB has formalized internal procedures for identifying and managing the verifications accounts (February 2020). DTMB will fully implement the internal procedures after migration to the State's Virtual Data Center (December 2020) to prevent duplication of efforts because automation changes will be required.

DTMB is unable to create separate verification accounts for MILogin administrators, within the MILogin Worker's Portal, due to technical limitations and costs. MILogin administrators each have a single account within the MILogin system for the MILogin Worker's Portal. These accounts are subscribed to multiple State Agency applications and are necessary for ongoing validation and troubleshooting purposes. Each subscription provides the MILogin administrator with a link to the Agency application. The MILogin system verifies the administrator's identify and passes the credentials to the Agency application. Neither the subscription or the credentials provide access to the Agency application. In cases where the MILogin administrator has access to an agency application, the Agency application administrator approved the access to the Agency application and created the user account within the Agency application.

Regarding part d. of the finding, DTMB disagrees DTMB is responsible for recertifying Agency application users and Agency Authorized Approvers. The SOM Technical Standard 1340.00.020.01 states the Agency information system owner is responsible for recertifying Agency application users. Recertifying of Agency Authorized Approvers is an Agency responsibility. To support State Agencies in recertifying Agency application users and authorized approvers, the MILogin team has an existing process to provide Agencies with a list of users and authorized approvers upon Agency request.

Finding #2 – Information System Security Plans Needed

DTMB agreed with the recommendation and continues to implement the State's Security Accreditation Program (MISAP) which the State began implementing in 2017. MISAP enables DTMB to identify and manage risks at an enterprise level.

DTMB agrees all information systems should have a System Security Plan (SSP) and an Authority to Operate (ATO) as outlined in SOM Technical Standard 1340.00.050.01. DTMB has developed and is implementing a prioritization for completing SSPs for State agency applications based on the criticality level of the applications. In addition, all new systems and systems with significant changes are completing SSPs and obtaining an ATO.

As part of the MISAP process, State agencies are required to assess the necessary security controls, including authentication, in accordance with the data classification and compliance

frameworks for Agency applications. The security assessment is approved by the State's Chief Security Officer and the Agency Authorizing Official.

The State has identified approximately 800 to 900 applications to complete SSPs, of which 169 have received an ATO as of mid-February 2020.

Finding #3 – Additional review of public user password and access controls

DTMB partially agreed with the recommendation.

MILogin is a gateway to State Agency applications for individuals and businesses doing business with or on behalf of the State of Michigan and State workers. MILogin currently supports approximately 5.4 million users and 266 Agency applications. Changes to the MILogin account and password parameters would have a significant impact on public users, and governmental and business services.

DTMB enables State Agencies to select various levels of gateway authentication for MILogin, such as ID Proofing and multifactor authentication, based on Agency identified business requirements as part of on-boarding an Agency application to MILogin and during the Agency application's lifecycle. These gateway authentications enable Agencies to add authentication controls prior to the Agency application-layer controls.

Regarding part a. of the finding, DTMB disagrees Citizen and 3rd Party Portal account and password parameters must be identical to the Worker's Portal. DTMB complies with SOM Technical Standard 1340.00.080.01 and recommendations in NIST 800-53 revision 4, which allows DTMB and State Agencies to establish different user account and password parameters for public users.

DTMB also disagrees it has not assessed the sufficiency of MILogin password and access controls for public users. DTMB has completed a risk assessment and received an ATO for the MILogin system. As part of this process, DTMB assessed the sufficiency of the password and access controls offered to State Agencies for public users. Additionally, as part of the State's ATO process, the State Agencies are required to identify the types of data their application contains as well as the sensitivity of the data. The sufficiency of password and access controls is assessed by each Agency Information System Owner and approved by the State's Chief Security Officer and the Agency Authorizing Official. All of these activities are led by DTMB to ensure State Agencies perform risk assessments for State Agency applications in accordance with SOM Technical Standard 1340.00.050.01.

Regarding part b. of the finding, DTMB is in the process of disabling the inactive accounts within the Citizen and Third Party Portal. DTMB anticipates disabling inactive Third Party accounts by the end of April 2020. DTMB will continue disabling inactive Citizen accounts and anticipates this will be completed in August 2020.

Finding #4 – Controls Needed to Ensure MILogin Availability

DTMB agreed with the recommendation.

Changes to SOM Technical Standard 1340.00.070.02 will impact all State Agencies and require careful consideration and planning. As such, DTMB continues to assess whether updates to the existing SOM Technical Standard are necessary, including conducting an impact assessment to determine the enterprise resources, funding requirements, and time necessary to implement changes. Upon completion of these activities, DTMB will determine whether updates to the existing SOM Technical Standard are necessary and the compliance date for the updated Standard.