STATE OF MICHIGAN

GRETCHEN WHITMER
GOVERNOR

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
LANSING

MICHELLE LANGE
DIRECTOR

January 3, 2024

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 48913

Dear Mr. Lowe:

In accordance with the State of Michigan, Financial Management Guide, part VII, 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 follow-up audit report of MiLogin (071-0570-18F).

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

Sincerely,

Michelle Lange
DTMB Director

c: Senator Sam Singh, Chair, Senate Oversight Committee
Senator Ed McBroom, Minority Vice Chair, Senate Oversight Committee
Senator John Cherry, Chair, Senate General Government Appropriations Subcommittee
Senator Thomas Albert, Minority Vice Chair, Senate General Government Appropriations Subcommittee
Representative Felicia Brabec, Chair, House General Government Appropriations Subcommittee
Representative Ann Bollin, Minority Vice Chair, House General Government Appropriations Subcommittee
Patti Tremblay, Executive Office of the Governor
Doug Ringler, Auditor General
Laura Clark, Chief Information Officer
Caleb Buhs, Chief Deputy Director
Jayson Cavendish, Chief Security Officer
Heather Frick, Director Agency Services
Jack Harris, Chief Technology Officer
Eric Swanson, Director Center for Shared Solutions
Sherri Irwin, Director of Office of Support Services, DTMB ICCO

Attachment

DTMB Corrective Action Plan for the OAG's MiLogin
follow-up audit (071-0570-18F)

Summary of Agency Responses to Recommendations

1. Audit recommendation DTMB partially agreed with and accepts the risk: 1a
2. Audit recommendation DTMB partially agreed with and is deferring to State Agencies for remediating: 1d

DTMB Responses to Recommendations:

Finding #1 – Improved Account Management and Monitoring Needed

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 authenticates a user's identity. The Agency application owners determine who has access to the Agency application and Agency application data and controls the activities users can perform within their applications.

Subpart a - DTMB partially agrees. Regarding subpart a. of the finding, as noted by the auditors in the previous audit, "*DTMB configured MiLogin to capture all auditable events*". The logged events are available for forensic after the fact review if necessary. While DTMB had not formalized the frequency DTMB would monitor logged events (which may be after the fact forensic review), DTMB accepts the residual risk, and meets the applicable State of Michigan Standard. DTMB has implemented processes to mitigate related risks, including:

- Forensic analysis tools to assist in monitoring MiLogin.
- State of Michigan (SOM) network accounts must use MFA if accessing the SOM network remotely.
- SOM Windows network accounts must use MFA to log into Office 365 services.
- State managed devices are managed for possible malware infections.
- Suspicious Windows account sign-in activity is monitored.
- Impossible Travel for Windows accounts is monitored.
- E-mail message size is limited.
- Access to Internet Personal Storage services is limited.
- Implementation of a tool to ensure non-authorized devices are not allowed access to the state's wired network.
- MiLogin uses privileged accounts to administer the application leveraging an enterprise tool which stores and manages administrative passwords. The tool automatically rotates the passwords at pre-defined intervals. The use of these accounts is logged.
- MiLogin also leverages another privileged access management tool which records events performed on the servers for forensic review as needed.

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 3:00 PM)

See Auditor's Comments in the audit report stating DTMB's response to part a. does not correlate to the identified issues.

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 3:00 PM)

The applicable SOM Technical Standard is 1340.00.040.01, specifically Control AU-2, which states: Determines, based on current threat information and ongoing assessment of risk, which events require auditing on a continuous basis and which events require auditing in response to specific situations.

Because DTMB has not formalized the frequency of its reviews and DTMB also stated that it does not review these logs for any unauthorized actions (only for health check reasons), then DTMB has not assessed which actions require continuous monitoring and which events require auditing in response to specific situations. Therefore, DTMB does not meet the applicable SOM Standard.

- MiLogin reviews DTMB MiLogin privileged accounts every 6 months to ensure the account is needed and appropriate for the privileged user's responsibilities.

- MiLogin utilizes a checklist process to offboard privileged user accounts to remove the account from the State of Michigan Active Directory and MiLogin.

Subpart d - DTMB partially agrees. DTMB agrees State Agencies are responsible for complying with State of Michigan Technical Security Standards and developing Agency level processes to implement the State of Michigan Technical Security Standards. In accordance with the State of Michigan Technical Security Standard 1340.00.020.01 Access Control Standard, each State agency is responsible for requiring approvals by an authorized requestor (AR) to create, modify, or delete information system accounts to their information systems. In addition, Agencies are responsible for recertifying their Agency information system accounts.

To support State Agencies in recertifying Authorized Approvers (AR), the MiLogin team has an existing process to provide Agencies with a list of Authorized Approvers upon Agency request. DTMB communicated to Agencies which currently use MiLogin, that the Agencies are responsible for keeping their Agency Authorized Approvers up to date and recertifying the Agency's Authorized Approvers with the MiLogin system (October 2023). Additionally, DTMB updated the MiLogin onboarding form to include a reminder that Agencies are responsible for keeping their Agency Authorized Approvers up to date and recertifying the Agency's Authorized Approvers with the MiLogin system (October 2023).

Comment on CAP from Michigan Office of the Auditor General (02/12/2024, 3:00 PM)

See Auditor's Comments in the audit report stating DTMB's response to part d. does not correlate to the identified issues.