Office of the Auditor General
Follow-Up Report on Prior Audit Recommendations

MILogin
Department of Technology, Management, and Budget

September 2023

State of Michigan Auditor General
Doug A. Ringler, CPA, CIA

071-0570-18F

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

The auditor general may make investigations pertinent to the conduct of audits.

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Follow-Up Report

MILogin

Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0570-18F

Released:
September 2023

We conducted this follow-up to determine whether DTMB had taken appropriate corrective measures in response to the material condition noted in our December 2019 audit report.

Prior Audit Information	Follow-Up Results		
	Conclusion	**Finding**	**Agency Preliminary Response**
Finding 1 - Material condition Improved account management and monitoring needed. Agency partially agreed.	Partially complied	Reportable condition exists. See Finding 1.	Partially agrees

Obtain Audit Reports

Online: audgen.michigan.gov

Phone: (517) 334-8050

Office of the Auditor General
201 N. Washington Square, Sixth Floor
Lansing, Michigan 48913

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General

This Page Left Intentionally Blank

OAG
Office of the Auditor General
Doug A. Ringler, CPA, CIA
Auditor General
201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • audgen.michigan.gov

September 15, 2023

Michelle Lange, Director
Department of Technology, Management, and Budget
and
Laura Clark, Chief Information Officer
Department of Technology, Management, and Budget
Elliott-Larsen Building
Lansing, Michigan

Director Lange and Chief Information Officer Clark:

This is our follow-up report on the material condition (Finding 1) and corresponding recommendation reported in the performance audit of MILogin, Department of Technology, Management, and Budget. That audit report was issued and distributed in December 2019. Additional copies are available on request or at audgen.michigan.gov.

Your agency provided the preliminary response included in this report. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

We appreciate the courtesy and cooperation extended to us during our follow-up. If you have any questions, please call me or Laura J. Hirst, CPA, Deputy Auditor General.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

MILOGIN

INTRODUCTION, PURPOSE OF FOLLOW-UP, AND SYSTEM DESCRIPTION

INTRODUCTION

This report contains the results of our follow-up of the material condition* (Finding 1) and corresponding recommendation reported in our performance audit* of MILogin, Department of Technology, Management, and Budget (DTMB), issued in December 2019.

PURPOSE OF FOLLOW-UP

To determine whether MILogin and DTMB had taken appropriate corrective measures to address our corresponding recommendation.

SYSTEM DESCRIPTION

MILogin is the State's enterprise solution for identity, credential, and access management. MILogin enables the State to establish and manage user identities and access across IT systems and applications.

MILogin functionality includes desktop and mobile single sign-on (SSO), identity federation, password management, identity proofing, and multi-factor authentication* (MFA) services. MILogin users include State employees, contractors, business partners, and citizens as well as other states and local units of government.

As of April 2023, MILogin had 306 links to IT systems and applications. Major agency systems utilizing MILogin include:

- DTMB's Statewide Integrated Governmental Management Applications (SIGMA)
- Michigan Department of Health and Human Services' (MDHHS's) Bridges Integrated Automated Eligibility Determination System (Bridges)
- MDHHS's Community Health Automated Medicaid Processing System (CHAMPS)
- MDHHS's Michigan Statewide Automated Child Welfare Information System (MiSACWIS)
- Michigan Department of Corrections' Offender Management System (OMS)
- Department of Treasury's Michigan Treasury Online (MTO) Web Portal

MILogin was implemented and supported by a third-party vendor. The vendor's contract expires in 2023 and has an estimated contract value of $77.6 million.

** See glossary at end of report for definition.*

DTMB's Cybersecurity and Infrastructure Protection is responsible for the direction and control of all MILogin implementation and operational activities, including those performed by the MILogin vendor.

PRIOR AUDIT FINDING AND RECOMMENDATION; AGENCY PLAN TO COMPLY; AND FOLLOW-UP CONCLUSION, RECOMMENDATION, AND AGENCY PRELIMINARY RESPONSE

FINDING 1

Audit Finding Classification: Material condition.

Summary of the December 2019 Finding:
DTMB, in conjunction with State agencies, did not fully establish and implement account management and monitoring controls over MILogin users.

Our review disclosed DTMB did not:

a. Fully monitor privileged MILogin activity.

b. Utilize unique administrative accounts for all administrative work.

c. Fully establish controls over test accounts utilized in the production environment.

d. Improve processes to recertify MILogin access.

Recommendation Reported in December 2019:
We recommended that DTMB, in conjunction with State agencies, fully establish and implement account management and monitoring controls over MILogin users.

AGENCY PLAN TO COMPLY*

On September 18, 2020, DTMB stated:

- Regarding part a. of the finding, DTMB agrees 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.

    - State of Michigan (SOM) Windows network accounts must use MFA if accessing the SOM network remotely.

    - SOM Windows network accounts must use MFA to log into Office 365 services.

** See glossary at end of report for definition.*

- State managed devices are managed for possible bot infections.
- Suspicious Windows account sign-in activity is monitored.
- Impossible Travel for Windows accounts is monitored.
- User 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 it has not fully established controls over accounts utilized in the MILogin production environment.

  DTMB does not agree the MILogin administrator accounts citied 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 portal, due to technical limitations and costs. MILogin administrators each have a single account within the MILogin system for the MILogin Worker 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 identity and passes the credentials to the agency application. Neither the subscription nor 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 any 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.

FOLLOW-UP CONCLUSION

Partially complied. A reportable condition* exists.

DTMB remediated parts b. and c. of this finding by updating its procedures for administrative accounts and reducing the number of validation accounts. For parts a. and d., DTMB did not perform any corrective action. Our follow-up noted DTMB had:

a. Not complied.

   DTMB informed us it accepted the risk and therefore did not take significant corrective action to fully monitor privileged MILogin activity.

b. Complied.

   According to SOM Technical Standard 1340.00.080.01, the information system uniquely identifies and authenticates system users. Also, unique identification of individuals in group accounts (such as shared privileged accounts) may need to be considered for detailed accountability of activity.

   DTMB implemented unique administrative accounts for all administrative work. Also, DTMB limited access to MILogin's default administrative account and increased accountability by requiring administrators to check out the password.

c. Substantially complied.

   DTMB reduced the number of validation accounts for two administrators from 57 and 75 agency applications to 0 and 12 agency applications, respectively. Also, these validation accounts do not perform testing in production.

d. Not complied.

   According to SOM Technical Standard 1340.00.020.03, DTMB is responsible for certifying compliance with established IT security policies, standards, and procedures. In addition, this Standard requires the

** See glossary at end of report for definition.*

agency to periodically reevaluate the access privileges granted to users and whether these privileges are still necessary to perform the user's job duties.

DTMB should communicate with agency application owners by routinely providing them a list of authorized requestors. This assists agency application owners in readily identifying and verifying their agency's authorized requestors who have the authority to approve access to agency applications.

FOLLOW-UP RECOMMENDATION

We recommend DTMB, in conjunction with State agencies, continue to fully establish and implement account management and monitoring over MILogin users.

FOLLOW-UP AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

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 application data.

Subpart a - DTMB partially agrees. Regarding part 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 has not formalized the frequency DTMB will monitor logged events (which may be after the fact forensic review), DTMB accepts the residual risk, while continuously seeking opportunities to improve future capability enhancements. 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.*

- *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.

State Agencies are responsible for complying with State of Michigan 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, Agencies are responsible for requiring approvals by an authorized requestor to create, modify, or delete information system accounts. In addition, Agencies are responsible for recertifying their Agency information system accounts.

DTMB will coordinate with the Agencies to determine a solution that ensures the Authorized Approvers and Authorization to Agency applications has appropriate review periods for validation of continued access entitlements. To support State Agencies in recertifying authorized business approvers, the MILogin team has an existing process to provide Agencies with a list of Authorized Business Approvers upon Agency request.

AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE*

DTMB's response indicated it partially agrees but identified no aspects in which it disagrees.

DTMB's response to part a. does not correlate to the identified issue. While there were several processes to monitoring privileged activity which occurred primarily at the operating system level, our finding relates to the lack of monitoring at the application level. For example, the processes noted by DTMB would not detect if an administrator made an unauthorized change to a user's MILogin account or MILogin functionality.

** See glossary at end of report for definition.*

Because privileged users have the ability to bypass established controls, it is important to monitor privileged activity at all levels.

DTMB's response to part d. does not correlate to the identified issue. The finding identified an opportunity for improved security to the SOM network by proactively providing data to its agency partners instead of waiting for them to request it.

FOLLOW-UP METHODOLOGY, PERIOD, AND AGENCY RESPONSES

METHODOLOGY

We reviewed DTMB's corrective action plan and new and updated policies and met with DTMB to discuss the status of its remediation efforts. Specifically, we:

- Met with MILogin staff to obtain an understanding of the implemented changes to:
  - Improve monitoring of MILogin privileged activity.
  - Utilize unique administrative accounts.
  - Establish controls over test accounts utilized in the production environment.
  - Improve processes to recertify MILogin access.
- Judgmentally sampled and reviewed 4 State employees' and 4 contractors' validation accounts.
- Reviewed processes for logging into the default administrative account.
- Reviewed the log-in report for the default administrative account.

PERIOD

Our follow-up generally covered July 1, 2022 through June 30, 2023.

AGENCY RESPONSES

Our follow-up report contains 1 recommendation. DTMB's preliminary response indicates it partially agrees with the recommendation.

The agency preliminary response following the follow-up recommendation in our report was taken from the agency's written comments and oral discussion at the end of our fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require an audited agency to develop a plan to comply with the recommendations and to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

GLOSSARY OF ABBREVIATIONS AND TERMS

agency plan to comply	The response required by Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100). The audited agency is required to develop a plan to comply with Office of the Auditor General audit recommendations and to submit the plan to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.
auditor's comments to agency preliminary response	Comments the OAG includes in an audit report to comply with *Government Auditing Standards*. Auditors are required to evaluate the validity of the audited entity's response when it is inconsistent or in conflict with the findings, conclusions, or recommendations. If the auditors disagree with the response, they should explain in the report their reasons for disagreement.
DTMB	Department of Technology, Management, and Budget.
IT	information technology.
material condition	A matter that, in the auditor's judgment, is more severe than a reportable condition and could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program. Our assessment of materiality is in relation to the respective audit objective.
MDHHS	Michigan Department of Health and Human Services.
multi-factor authentication (MFA)	An authentication method in which a user is granted access only after successfully presenting two or more authentication factors.
OAG	Office of the Auditor General.
performance audit	An audit that provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision-making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.

reportable condition	A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: a deficiency in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; opportunities to improve programs and operations; or fraud.
SOM	State of Michigan.
SSO	single sign-on.

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8070