Office of the Auditor General
Performance Audit Report

MILogin
Department of Technology, Management, and Budget

December 2019

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

071-0570-18

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

Performance Audit

MILogin

Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0570-18

Released:
December 2019

MILogin is the State's identity, credential, and access management system. MILogin was implemented in October 2014. 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, identity federation, password management, identity proofing, and multi-factor authentication services. MILogin users include State employees, contractors, business partners, and citizens as well as other states and local units of government. DTMB's Center for Shared Solutions is responsible for the integration and operation of MILogin. As of October 2019, MILogin had 227 links to IT systems and applications.

Audit Objective	Conclusion
Objective #1: To assess the effectiveness of controls over MILogin administration and end user account management.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
MILogin privileged activity was not sufficiently monitored, unique accounts were not used for all administrative work, and test accounts were not adequately controlled. Also, improvements would occur with periodic recertification of agency authorized approvers and user authorizations (Finding #1).	X		Partially agrees
DTMB, in conjunction with State agencies, should ensure that all information systems utilizing MILogin have a system security plan and an authorization to operate. Fifty-three percent of systems sampled appeared to require a higher authentication level based on the agency's reported data classification level (Finding #2).		X	Agrees
For public users, DTMB should assess the need to update certain MILogin security parameters. MILogin's automated controls did not function as intended for certain accounts (Finding #3).		X	Partially agrees

Audit Objective	Conclusion
Objective #2: To assess the effectiveness of DTMB's efforts to ensure that MILogin properly authorizes application access.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
See Finding #1, part d. and Finding #2, part a. (2).			

Audit Objective	Conclusion
Objective #3: To assess the effectiveness of DTMB's controls to ensure the availability of MILogin.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
MILogin backup files were not always created, disaster recovery plans were not fully tested, and vulnerability scans were not always run (Finding #4).		X	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

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

December 27, 2019

Ms. Tricia L. Foster, Director
Department of Technology, Management, and Budget
Lewis Cass Building
Lansing, Michigan

Dear Ms. Foster:

This is our performance audit report on MILogin, Department of Technology, Management, and Budget.

We organize our findings and observations by audit objective. Your agency provided the preliminary responses to the recommendations at the end of our fieldwork. 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 this audit.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

MILOGIN

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

ADMINISTRATION AND END USER ACCOUNT MANAGEMENT

BACKGROUND

Identity management is a set of security practices that allow an organization to enable the right individuals to access the right IT resources* at the right time for the right reasons.

Identity is a set of characteristics that describe an individual or other account representing a service, device, or application. A person's name is often used as his/her identity. However, because there can be multiple people with the same name, authentication* is used to uniquely identify a person.

Identity management systems typically utilize three types of authentication factors* to verify a user's identity. The three factors are:

- Something you know such as a password or personal identification number (PIN).
- Something you have such as a smart card or identification card.
- Something you are such as a fingerprint or other biometric identifier.

For systems that are sensitive or high risk, additional authentication methods, such as multi-factor authentication* (MFA) or identity proofing*, may be required. MFA requires the user to utilize two or more of the above authentication methods to access the system. Identity proofing is the process of verifying a person's identity before issuing him/her an account. Typically, identity proofing is performed over the Web or through a call center and requires the individual to correctly answer several life history or transaction questions obtained from public or proprietary data sources. Identity proofing can also occur during a face-to-face interaction.

Other features provided by identity and access management systems include single sign-on (SSO) and federation*. SSO allows users to authenticate once and access other associated applications. Federation allows an organization to trust users' identity and access information when authenticated by another organization.

AUDIT OBJECTIVE

To assess the effectiveness of controls over MILogin administration and end user account management.

CONCLUSION

Moderately effective.

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

FACTORS IMPACTING CONCLUSION

- The Department of Technology, Management, and Budget (DTMB) established and implemented policies for identity, credentialing, and access management.

- Material condition* related to improved account management and monitoring (Finding #1).

- Reportable conditions* related to the need for information system security plans and assessing password and access controls for public users (Findings #2 and #3).

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

FINDING #1

Improved account management and monitoring needed.

DTMB, in conjunction with State agencies, did not fully establish and implement account management and monitoring controls over MILogin users. Implementing additional controls would promote the principle of least privilege* and reduce the risk of unauthorized access to MILogin and the information systems utilizing MILogin.

State of Michigan (SOM) Technical Standards 1340.00.020.01 and 1340.00.040.01 require State agencies to ensure that users of the State's information systems are granted only the minimum access necessary to accomplish assigned tasks in accordance with the roles and responsibilities of their job functions. The standards also require periodic review of access rights for appropriateness and the monitoring of privileged user activity.

Our review disclosed that DTMB did not:

Monitoring of MILogin administrators was not sufficient.

a. Fully monitor privileged MILogin activity.

   For example, MILogin's application administrators are in sensitive positions and have elevated access rights to perform their job responsibilities, such as to configure MILogin functionality. Because of their access and expertise, the application administrators have the knowledge and ability to circumvent established controls and conceal their activities. As such, it is important for MILogin management to identify and monitor privileged activity. Examples of MILogin privileged activity that should be monitored include:

   - Creation of a user by an administrator.
   - User locked by an administrator.
   - User unlocked by an administrator.
   - Administrator commands that resulted in a modification of MILogin functionality.

   DTMB configured MILogin to capture all auditable events and informed us that it forwarded its logs to the State's Security Information Event Management systems. In addition, DTMB informed us that it received alerts for certain security related events. However, the alerts were for activities impacting the operating system and did not relate to privileged MILogin activity. MILogin management had not established sufficient monitoring to detect if administrators misused their privileged access*. DTMB informed us that it needs additional resources and tools to improve its ability to effectively and efficiently monitor privileged users.

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

Some administrative work was performed with a shared account.

b. Utilize unique administrative accounts for all administrative work.

   For certain MILogin functions, administrators performed their work utilizing MILogin's default administrative account. The account allows users full control over one of the MILogin components that controls access to agency applications. Individual accounts would allow DTMB to establish accountability for each administrator's actions and help mitigate the risk that unauthorized activity may not be detected in a timely manner.

   Upon bringing this matter to management's attention, DTMB informed us that it began testing a solution to create individual administrative accounts and manage changes to the default account password.

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

   If not properly managed, the use of test accounts in production environments may create a security risk because the accounts may inadvertently be granted application access, may not be disabled when no longer needed, or may not be properly monitored.

   Although SOM Technical Standard 1360.00.10 requires the removal of all test accounts prior to production, DTMB informed us that the test accounts were required to ensure that MILogin functioned properly. For example, MILogin administrators used test accounts to validate MILogin functionality after configuration changes were made to the system and to perform daily health checks of MILogin connectivity. In addition, DTMB informed us that when integrating new applications, for certain features, multiple accounts were required to properly test MILogin.

   However, DTMB had not established standards for identifying, managing, and monitoring test accounts. In addition, MILogin administrators used their SOM accounts instead of easily identifiable test accounts to test MILogin functionality. For example, our review disclosed:

   - 6 (35%) of 17 judgmentally sampled agency applications had test accounts that were active in the agency's application. We did not perform additional procedures to determine the level of application access of the test accounts.

   - In the Worker portal, we identified administrators with a high number of test accounts. For example, we identified two administrators with test accounts for 57 and 75 agency applications.

- One application, in the Third-Party portal, had multiple administrators with test accounts. Although most of the administrators had a single account, two of the administrators had 19 and 17 test accounts.

According to the Cloud Security Alliance* (CSA), the use of test accounts in Web applications, such as MILogin, are needed to test functionality and cannot be completely removed. Therefore, CSA recommends that organizations implement the following best practices:

- Ensure that test accounts are assigned the least possible privileges.

- Establish an end date for the test accounts and establish controls to ensure that the test accounts are only active when needed.

- When possible, automate testing to eliminate the need for individual test accounts.

- Adopt a common syntax to identify test accounts (test_* ,* 12345, #username).

- Monitor test account activities to ensure that test accounts are not used for production transactions.

In addition, because State agencies are responsible for ensuring that test accounts are not inadvertently granted application access privileges, DTMB should formally identify MILogin test accounts and communicate the application owner's responsibilities for disabling and/or monitoring test account activity.

d. Improve processes to recertify MILogin access.

Specifically, DTMB and State agencies should:

(1) Establish and implement procedures to recertify agency authorized approvers.

Authorized approvers are responsible for approving requests for agency application access. For five judgmentally sampled applications, we asked State agencies to verify their application's authorized approvers. Four (80%) of the 5 State agencies identified at least one authorized approver with the ability to approve access requests who no longer had that responsibility or was no longer employed by the agency.

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

(2) Enhance communication with agency application owners regarding application owners' responsibilities for managing users' access to their applications. To remove a user's access to his/her application, agencies are responsible for submitting a request for change to MILogin management. To assist agencies, DTMB informed us that it could provide, upon request, a listing of users with application access.

This finding represents a material condition primarily because of the lack of monitoring and accountability for all privileged administrative accounts. Privileged accounts are the most powerful and, if compromised or abused, could create a security risk.

RECOMMENDATION

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

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB partially agrees 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 application data.

Regarding part a. of the finding, DTMB partially 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. DTMB has implemented processes to reduce risks, such as:

- *Forensic analysis tools to assist in monitoring MILogin administrator activities.*
- *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.*

DTMB will need additional resources, including funding and tools, to expand its monitoring of privileged users. DTMB will reassess this in future budget cycles.

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

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

DTMB does not agree that the MILogin administrator accounts cited in the OAG's audit report are test accounts; the accounts are verifications accounts used by DTMB to perform validation of MILogin system functionality and perform daily health checks, in accordance with SOM Technical Standard 1340.00.060.04. DTMB will formalize internal procedures for identifying and managing the verification accounts (March 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 Workers Portal, due to technical limitations and costs. MILogin administrators each have a single account within the MILogin system for the MILogin Workers' 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 or the credentials provide access to the Agency application or access to data within 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 that the MILogin team 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. Recertification 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.

AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE*

MILogin is more than a gateway to agency applications. It provides key access controls that ensure that an application's users are properly authenticated, thereby ensuring that only authorized users have access to agency applications and data.

DTMB's response to part a. identified several processes to monitor privileged activity that occur 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. Because privileged users have the ability to bypass established controls, it is important to monitor privileged activity at all levels.

DTMB disagrees that the administrator accounts cited in part c. are test accounts and considers them to be verification accounts that it uses to validate system functionality and perform daily health checks. We consider verification accounts to be a type of test account. The best practices identified in the finding specifically address the risks associated with the need to use test accounts in a production system to test system functionality. Also, regarding administrator accounts in the Worker portal, SOM Technical Standard 1345.00.30 provides for special use accounts that could be used for audit, testing, or other purposes.

DTMB disagrees that it is responsible for recertifying agency application users and approvers. DTMB cited SOM Technical Standard 1340.00.020.01 that states that the information system owner is responsible for recertifying Agency application users. DTMB is the MILogin application owner and, therefore, is responsible for recertifying agency authorized approvers.

Therefore, the finding stands as written.

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

FINDING #2

Information system security plans needed.

DTMB, in conjunction with State agencies, should ensure that all information systems utilizing MILogin have a system security plan (SSP) and an authorization to operate (ATO). An SSP and ATO diminish the risk that systems may not be utilizing the appropriate level of authentication or be fully secured.

SOM Technical Standards 1340.00.050.01 and 1340.00.150.01 require that all information systems have risk and security assessments to determine the effectiveness of security controls.

The Standards require DTMB and the system's business owner to develop an SSP and a plan of action and milestones to correct identified control weaknesses and reduce or eliminate known system vulnerabilities. Upon completion of the SSP, the State's chief information officer and the information system's authorizing official* formally authorize the system for operation by ensuring that the system is properly categorized, approving the security assessment and controls, and assuming responsibility for any residual risks.

The Standards require that new systems be authorized before they are placed in operation and that system owners obtain an updated security authorization at least every three years; when a significant change occurs to the system, such as integration of the system with MILogin; or when the classification of data processed by the system changes.

DTMB informed us that, when it integrated some systems with MILogin, its processes for conducting security assessments were less formalized. As a result, we were unable to determine whether DTMB, in conjunction with State agencies, had fully implemented appropriate controls. For example:

a. For 19 judgmentally selected agency systems, we identified systems that appeared to require a higher level of authentication than what was implemented and systems that did not utilize MILogin's security features. Specifically:

   (1) 10 (53%) systems appeared to require a higher authentication level based on the agency's reported data classification level. SOM Technical Standard 1340.00.080.03 establishes authentication levels based on a system's data classification. According to the Standard, as risk increases because of the sensitivity of electronic transactions, the level of confidence in the credential used to access the information must also increase. Although all 10 information systems required the use of a unique username and password, additional verification such as identity proofing or MFA should be used based on the system's data classification.

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

(2) 7 (37%) systems did not display a login warning banner in MILogin. SOM Technical Standard 1430.00.020.01 requires the display of a warning banner before granting access. Warning banners provide legal notice to intruders that certain types of activities are illegal and advise authorized and legitimate users of their obligations related to acceptable use.

DTMB informed us that some of the required controls, such as login warning banners or identity proofing, may be implemented in the information system rather than in MILogin.

b. 12 (8%) of 153 system links did not use in-transit encryption between MILogin and the system in accordance with SOM Technical Standard 1340.00.170.03 or have a documented Technical Review Board exception. Using the appropriate level of encryption minimizes the likelihood that sensitive or confidential information will be inadvertently disclosed or accessed during transmission.

Performing risk and security assessments would ensure that key controls are properly documented, control weaknesses and security vulnerabilities are properly remediated, and residual risks are formally accepted.

RECOMMENDATION

We recommend that DTMB, in conjunction with State agencies, ensure that all information systems utilizing MILogin have an SSP and ATO.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation. DTMB will continue implementing the State's Security Accreditation Program (MISAP) which the State began implementing in 2017 and continues to mature.

DTMB agrees that all information systems should have an SSP and ATO as outlined in SOM Technical Standard 1340.00.050.01. DTMB has developed 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.

The State of Michigan is a nationwide leader for implementing an enterprise approach to performing risk assessments on State agency applications and issuing ATOs. DTMB modeled MISAP after the federal Department of Defense's system application accreditation and certification process. MISAP enables DTMB to identify and manage risks at an enterprise level.

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 agency authorizing official.

The State has identified approximately 800 to 900 applications to complete SSPs, of which 164 have received an ATO.

FINDING #3

Additional review of public user password and access controls needed.

DTMB needs to assess the sufficiency of MILogin password and access controls* for public users. Implementing strong password and access controls helps ensure that critical systems are protected from unauthorized use or disruption and that sensitive data, such as taxpayer data, medical records, and other personally identifiable information, is not inappropriately viewed, added, deleted, copied, disclosed, or modified.

DTMB Administrative Guide to State Government policy 1340.00 adopts National Institute of Standards and Technology* (NIST) Special Publication 800-53 as the minimum security controls over the State's information systems. DTMB has established policies, procedures, and standards to implement the security controls. Exceptions must be approved by the Enterprise Technical Review Board.

Our review of MILogin configurations and user account records disclosed:

a. For the Citizen and Third-Party portals, DTMB did not configure MILogin user account and password parameters to meet the same security standards as those required for State employees using the Worker portal.

   SOM Technical Standard 1340.00.080.01 allows DTMB and State agencies to establish different user account and password parameters for public users. However, for systems containing federal data, the standard requires a risk assessment to ensure that the public's ease of use is balanced with appropriate security to mitigate risks.

   DTMB informed us that the configuration settings for the Citizen and Third-Party portals were inherited from the State's legacy SSO system and that at the time of MILogin's implementation, management's focus was on the public's ease of use.

   Because MILogin controls access to information systems containing federal and other sensitive data, we requested DTMB's risk assessment regarding how it determined the user account and password settings for MILogin's public portals. DTMB was unable to provide its risk assessment and informed us that it was the responsibility of each State agency to determine which MILogin solution provided the appropriate level of authentication and security for its applications.

   However, as noted in Finding #2, at the time MILogin was implemented, DTMB's processes for conducting security assessments were not mature. Consequently, DTMB and State agencies had not ensured that all systems utilizing

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

MILogin had an SSP and ATO. As such, a risk exists that agencies with systems containing federal and other sensitive or confidential data have not sufficiently evaluated the need for additional authentication controls, such as MFA. As a result, the less restrictive user account and password controls for public users may pose an unacceptable risk for those applications requiring a higher level of authentication.

Furthermore, IT security threats and standards have evolved since MILogin's implementation in October 2014. As such, DTMB should assess whether the current balance of security controls compared with the public's ease of use is sufficient to protect against account compromise and unauthorized access.

Because of the confidentiality of these configurations, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to DTMB.

b. DTMB should enhance its change control processes to ensure that all MILogin accounts affected by system modifications are identified and corrected. Because DTMB did not identify and correct all accounts impacted by system modifications, MILogin's automated controls did not function as intended for certain accounts. Because of the confidentiality of these controls, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to DTMB.

Correcting all accounts impacted by system modifications would help ensure that all MILogin accounts follow established business rules and help DTMB and State agencies reduce the risk that an unauthorized user could exploit the account.

RECOMMENDATION

We recommend that DTMB assess the sufficiency of MILogin password and access controls for public users.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB partially agrees 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 currently supports 5.4 million users and 263 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 that Citizen and 3rd Party portals account and password parameters must meet the same security standards as 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 that 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.

DTMB continues to lead a Statewide effort to ensure that State Agencies perform risk assessments for State Agency applications in accordance with SOM Technical Standard 1340.00.050.01. As part of this process, the State Agencies are required to identify the types of data their application contains as well as the sensitivity of this data. Also, 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.

DTMB disagrees that the MILogin team is responsible for identifying appropriate access and security controls, including account and password parameters, for State Agencies' applications. State Agencies are responsible for assessing and identifying the necessary controls based on the type of data within the State Agency's application.

Regarding part b. of the finding, DTMB agrees and will complete corrections of all remaining accounts impacted by system migrations to MILogin (April 2020).

AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE

Although SOM technical standards allow DTMB to establish separate security standards for the public and State employees, the standards also require DTMB to perform a risk assessment to balance the public's ease of use with appropriate security to mitigate risks. In November 2018, DTMB provided us its draft MILogin system security plan. Although the plan acknowledged the differences between public and worker security parameters identified by the audit, the plan did not describe DTMB's basis for implementing less stringent public security settings.

Because some agency applications inherit certain security controls from MILogin, it is possible that an application may have different security controls for public users and State employees accessing the same transactions and data.

DTMB also disagreed that the MILogin team is responsible for identifying appropriate access and security controls for State agencies' applications. Our finding is not directed to the MILogin team but to DTMB. According to SOM Administrative Guide to State Government policies 1305.00 and 1340.00, DTMB is responsible for establishing enterprise policies, procedures, and standards to protect SOM information. State agencies are required to establish and implement procedures to enforce DTMB policies and may implement more stringent security controls in conjunction with DTMB.

Therefore, the finding stands as written.

AUTHORIZATION OF APPLICATION ACCESS

BACKGROUND

Authorization* is the process of granting or denying access to an IT resource such as an application or database based on a user's identity. In addition, authorization determines a user's access rights and privileges after being allowed into the system. For example, a user's authorizations will determine what system functions and features are available and the type of access, such as read, update, or delete.

MILogin provides coarse-grained authorization*, which controls whether an individual has access to an application. After access to the application has been granted, State agencies are responsible for managing users' access rights and privileges within their applications.

AUDIT OBJECTIVE

To assess the effectiveness of DTMB's efforts to ensure that MILogin properly authorizes application access.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- DTMB, in conjunction with State agencies, established processes for approving user requests for agency application access.
- Material condition related to periodic recertification of agency authorized requestors responsible for approving requests for agency application access (Finding #1, part d.).
- Reportable condition related to displaying login warning banners (Finding #2, part a. (2)).

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

AVAILABILITY OF MILOGIN

BACKGROUND

Information has value only if the right people can access it when the information is needed. Availability* controls help ensure that applications and data are available when needed regardless of the adverse circumstances that an organization may face.

DTMB designed MILogin to ensure high availability* because MILogin's availability directly impacts access to critical agency information systems.

Some of the key controls to help ensure high availability include:

- Duplicate network communication paths and system processing across multiple locations.
- Redundant hardware and software that will immediately take over operation in the event of a failure.
- Regular off-site backups.
- Comprehensive disaster recovery (DR) planning and testing.

AUDIT OBJECTIVE

To assess the effectiveness of DTMB's controls to ensure the availability of MILogin.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- MILogin architecture was designed to provide high availability.
- Documented DR plan and monthly failover* testing.
- Monthly vulnerability scans were performed for MILogin servers.
- Reportable condition related to enhancing controls to ensure MILogin availability (Finding #4).

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

FINDING #4

DTMB should continue to enhance controls designed to ensure that MILogin is available to authorized users when needed.

Controls needed to ensure MILogin availability.

Threats impacting MILogin availability may be intentional or unintentional in nature and can occur for a number of reasons, including malicious attackers attempting to bring down the MILogin Web site or hardware failure such as hard drive or power supply failure.

Our review of selected controls related to backup, DR, and vulnerability scans disclosed that:

a. DTMB had not implemented effective monitoring processes to ensure that the Backup Team always identified failed backups and documented the corrective action taken. As a result, DTMB cannot ensure that all failed backups were identified in a timely manner and appropriate corrective action was taken.

   We reviewed backup logs from October 2016 through August 2018 for 22 MILogin hosts and identified 20 days on 9 of the hosts in which the backup software did not run and backup files were not created. DTMB was unable to locate documentation of its actions to identify and remediate the failures. Also, we judgmentally sampled 17 instances in which the backup of a host failed on two or more consecutive days, according to the backup log. For 5 (29%) of the 17 instances, DTMB was unable to locate documentation of its actions to identify and remediate the failure.

   After bringing this matter to DTMB's attention, the Backup Team formalized its procedures for monitoring failed backups.

b. DTMB should expand its testing of the MILogin DR plan to ensure that the system can be recovered quickly and efficiently in the event of a major disruption of service.

   MILogin includes redundant hardware and software to ensure a high uptime rate without interruption. In the event that one component of MILogin fails, the system should failover to the remaining components so that the system still functions.

   According to the *Disaster Recovery Journal*, a high availability system is not protected from failures caused by cyber attacks, which require an organization to go back to a certain point in time to recover data. Although DTMB conducted full monthly failover tests, additional DR plan testing would help DTMB identify potential DR plan deficiencies and evaluate the ability of recovery personnel to implement the plan in an effective and efficient manner.

Best practices for DR testing suggest that organizations begin with a "tabletop" walk through of the plan and related recovery procedures and eventually incorporate more complex operational, technical, and staff-related scenarios such as:

- Loss of key personnel responsible for recovery efforts.
- Use of backup files to recover from a denial of service, ransomware, or other cyber attack.

c. DTMB should ensure that monthly vulnerability scans are completed for all active MILogin appliances*.

Vulnerability scanning is a key component of the State's Enterprise Vulnerability Management (EVM) Program. EVM is a cyclical process of identifying, classifying, and remediating vulnerabilities.

We reviewed documentation of DTMB's monthly MILogin vulnerability scans from October 2016 to September 2018. In addition, we evaluated the timeliness of DTMB's remediation of vulnerabilities between April 2018 and September 2018.

DTMB ensured that all MILogin servers received monthly vulnerability scans. However, for certain MILogin appliances, DTMB should:

(1) Utilize scanning tool capabilities to monitor for instances when scheduled scans were not successfully completed.

(2) Ensure the successful completion of vulnerability scans when additional Internet Protocol (IP) addresses are enabled.

DTMB informed us that, as of May 2019, vulnerability scans were completed for all active appliance IP addresses.

RECOMMENDATION We recommend that DTMB continue to enhance controls designed to ensure that MILogin is available to authorized users when needed.

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

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation.

DTMB adheres to SOM Technical Standard 1340.00.070.02 which requires annual disaster recovery testing. The Standard allows for:

- *A walk-through of the disaster recovery plan.*
- *Tabletop testing of a simulated disaster.*
- *Partial testing to validate that business transactions can be performed successfully, or*
- *Full cutover testing to verify if recovery systems can assume the full production workload.*

DTMB constantly strives to enhance controls designed to ensure that MILogin is available to authorized users. DTMB will evaluate the OAG's recommendations and consider potential updates to relevant SOM policies, standards, and procedures.

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 SSO, identity federation, password management, identity proofing, and MFA services. MILogin users include State employees, contractors, business partners, and citizens as well as other states and local units of government.

As of October 2019, MILogin had 227 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 Child Welfare Information System (MiSACWIS)
- Michigan Department of Corrections' Offender Management Network Information System (OMNI)
- 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 $69.4 million.

DTMB's Center for Shared Solutions is responsible for the direction and control of all MILogin implementation and operational activities, including those performed by the MILogin vendor.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine the program and other records related to MILogin. We conducted this performance audit* in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The following IT general controls were excluded from the scope of the audit: system development, configuration management, and access controls over the MILogin operating system and database. In addition, we excluded controls inherited from Active Directory.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 2016 through December 2018 and May 2019, when we obtained data used to evaluate user access and validate MILogin configurations.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of MILogin. During our preliminary survey, we:

- Obtained an understanding of the MILogin system architecture.
- Identified the agencies and applications that use MILogin.
- Reviewed the contract for MILogin development, maintenance, and operations.
- Reviewed SOM IT technical policies, standards, and procedures for MILogin. We also reviewed industry best practices related to SSO and identity and access management, including NIST and Control Objectives for Information and Related Technology* (COBIT).
- Interviewed DTMB and contracted personnel responsible for MILogin processes for establishing application access and other processes including help desk functions, administrative access, vulnerability scans, and system backup.

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

OBJECTIVE #1

To assess the effectiveness of controls over MILogin administration and end user account management.

To accomplish this objective, we:

- Judgmentally sampled 19 of 190 agency application links, as of August 2018, and compared the application's authentication level and data classification with the SOM Identity, Credentialing, and Access Management Standard. Because we used a judgmental sample, we could not project our results to other applications.
- Reviewed selected controls over the granting and monitoring of MILogin privileged access.
- Reviewed selected end user security configurations related to user accounts and passwords.

OBJECTIVE #2

To assess the effectiveness of DTMB's efforts to ensure that MILogin properly authorizes application access.

To accomplish this objective, we:

- Judgmentally sampled 19 of 190 agency application links as of August 2018 to assess whether MILogin workflows were designed to ensure that user access requests were properly approved.
- Validated authorized requestors for 5 of 19 judgmentally sampled agency applications selected above.

Because we used judgmental samples, we could not project our results to other applications.

OBJECTIVE #3

To assess the effectiveness of DTMB's controls to ensure the availability of MILogin.

To accomplish this objective, we:

- Evaluated the sufficiency of the System and Organization Controls (SOC) 2 report* for the State's co-location data center*. The SOC 2 report covered the period of October 1, 2016 through September 30, 2017.
- Evaluated DTMB's vulnerability scanning from October 2016 to September 2018 and remediation efforts from April 2018 to September 2018.
- Reviewed the MILogin backup and recovery processes.
- Reviewed the sufficiency of MILogin's DR plan and recovery testing.

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

CONCLUSIONS

We base our conclusions on our audit efforts and any resulting material conditions or reportable conditions.

When selecting activities or programs for audit, we direct our efforts based on risk and opportunities to improve State government operations. Consequently, we prepare our performance audit reports on an exception basis.

AGENCY RESPONSES

Our audit report contains 4 findings and 4 corresponding recommendations. DTMB's preliminary response indicates that it agrees with 2 recommendations and partially agrees with 2 recommendations.

The agency preliminary response that follows each recommendation in our report was taken from DTMB'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

access controls	Controls that protect data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.
appliance	A computer with software or firmware that is specifically designed to provide a specific computing resource. Unlike general purpose computers, appliances are generally not designed to allow the customer to change the software and the underlying operating system or to flexibly reconfigure the hardware.
ATO	authorization to operate.
auditor's comments to agency preliminary response	Comments that 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.
authentication	Verification of the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.
authentication factor	A category of credential that is intended to verify, sometimes in combination with other factors, that entities requesting access to a system are who or what they are declared to be. The three types of authentication factors are something you know, something you have, and something you are.
authorization	The concept of allowing access to resources only to those permitted to use them.
authorizing official	An individual with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to the organization's operations. Because of the responsibility of this role, the authorizing official must be a State of Michigan executive responsible for the business operations supported by the system.
availability	Timely and reliable access to data and information systems.
Cloud Security Alliance (CSA)	Promotes the use of best practices for providing security assurance within cloud computing and provides education on the uses of cloud computing to help secure all other forms of computing.

coarse-grained authorization	The allowing or disallowing of access to a resource as opposed to access within the resource. MILogin provides user links to agency applications. MILogin verifies user identity and passes the user's credentials to the application. Access within the application is granted by the agency application owner.
co-location data center	A facility in which a business can rent space for servers and other computing hardware. Typically, a co-location data center provides the building, cooling, power, bandwidth, and physical security while the customer provides servers and storage.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines published by the IT Governance Institute as a generally applicable and accepted standard for good practices for controls over IT.
DR	disaster recovery.
DTMB	Department of Technology, Management, and Budget.
EVM	Enterprise Vulnerability Management.
failover	In the event that one component of a system fails, the system transfers functions to the remaining components so that the system remains available to users.
federation	A process that allows an organization to accept identity and access information across organizational boundaries based on trust.
high availability	A system that has been designed to operate continuously without interruption to service.
identity proofing	Verification of a person's identity before an organization issues them accounts and credentials. Verification is based on life history or transaction information obtained from public and proprietary data sources.
IP	Internet Protocol.
IT	information technology.
IT resources	Hardware, software, and other equipment such as an application, network device, server, or workstation.

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.
National Institute of Standards and Technology (NIST)	An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs.
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.
PIN	personal identification number.
principle of least privilege	The practice of limiting access to the minimal level that will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user access rights that they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes.
privileged access	Extensive system access capabilities granted to persons responsible for maintaining system resources. This level of access is considered high risk and must be controlled and monitored by management.
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: an opportunity for improvement within the context of the audit

	objectives; a deficiency in internal control that is significant within the context of the audit objectives; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely to have occurred.
SOM	State of Michigan.
SSO	single sign-on.
SSP	system security plan.
System and Organization Controls (SOC) report	Designed to help organizations that provide services to user entities build trust and confidence in their delivery processes and controls through a report by an independent certified public accountant (CPA). Each type of SOC report is designed to meet specific user needs: • SOC 1 (Report on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting) - Intended for user entities and the CPAs auditing their financial statements in evaluating the effect of the service organization's controls on the user entities' financial statements. • SOC 2 (Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy) - Intended for a broad range of users that need information and assurance about a service organization's controls relevant to any combination of the five predefined control principles. There are two types of SOC 1 and SOC 2 reports: o Type 1 - Reports on the fairness of management's description of a service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description, as of a specified date. o Type 2 - Includes the information in a type 1 report and also addresses the operating effectiveness of the controls to achieve the related control objectives included in the description, throughout a specified period. • SOC 3 (Trust Services Report for a Service Organization) - Intended for those needing assurance about a service organization's controls that affect the security, availability, or processing integrity of the systems a service organization

employs to process user entities' information, or the confidentiality or privacy of that information, but do not have the need for or the knowledge necessary to make effective use of a SOC 2 report.

- SOC for Cybersecurity. Intended to communicate relevant information about the effectiveness of an organization's cybersecurity risk management programs.

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8060, Ext. 1650