Office of the Auditor General
Performance Audit Report

Selected Community Health-Related IT Systems

Michigan Department of Health and Human Services and
Department of Technology, Management, and Budget

March 2023

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

391-0593-22

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
Selected Community Health-Related IT Systems
Michigan Department of Health and Human Services (MDHHS) and Department of Technology, Management, and Budget (DTMB)

Report Number:
391-0593-22

Released:
March 2023

MDHHS uses more than 80 IT systems to collect and report community health-related information. Our scope included the following four systems: Michigan Disease Surveillance System, Newborn Screening Laboratory Information Management System, Bureau of Laboratories Laboratory Information Management System, and Vital Event Registration Application. MDHHS uses these systems to collect and report birth information, infectious disease monitoring and tracking data, newborn health information, and other health data reported to entities such as the Centers for Disease Control and Prevention. MDHHS has primary responsibility for establishing, maintaining, and monitoring internal control over its critical IT applications. DTMB has the primary responsibility for designing, implementing, and executing IT general controls.

Audit Objective	Conclusion
Objective: To assess the sufficiency of MDHHS's and DTMB's security and user access controls over selected community health-related IT systems.	Not sufficient for MDHHS Sufficient, with exceptions, for DTMB

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
Deficiencies in security and access controls, in conjunction with a lack of monitoring, resulted in a high level of risk that sensitive data was potentially exposed to a data breach (Finding 1).	X		Agree
All four systems lacked effective processes for granting and removing access, annually recertifying appropriateness of users' roles and permissions, and ensuring appropriateness of security configuration settings. The systems also lacked sufficient documentation of MDHHS's role compatibility review (Finding 2).	X		Partially agree

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

March 31, 2023

Ms. Elizabeth Hertel, Director
Michigan Department of Health and Human Services
South Grand Building
Lansing, Michigan
and
Ms. Michelle Lange, Director
Department of Technology, Management, and Budget
and
Ms. Laura Clark, Chief Information Officer
Department of Technology, Management, and Budget
Elliott-Larsen Building
Lansing, Michigan

Dear Ms. Hertel, Ms. Lange, and Ms. Clark:

This is our performance audit report on the Selected Community Health-Related IT Systems, Michigan Department of Health and Human Services and Department of Technology, Management, and Budget.

Your agency provided 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

SELECTED COMMUNITY HEALTH-RELATED IT SYSTEMS

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

SELECT SECURITY AND ACCESS CONTROLS

BACKGROUND

Security* controls are the management, operational, and technical controls designed to protect the availability*, confidentiality*, and integrity* of a system and its information.

Access controls* limit or detect inappropriate access to computer resources, thereby protecting the resources from unauthorized modification, loss, and disclosure. For access controls to be effective, they should be properly authorized, implemented, and maintained.

The Michigan Department of Health and Human Services (MDHHS) uses more than 80 IT systems to collect and report community health-related information. We conducted an assessment and identified the following systems to review based on risk factors such as the system's downtime; impact on citizens' health and safety; and data confidentiality, integrity, and availability:

- Michigan Disease Surveillance System (MDSS)
- Newborn Screening Laboratory Information Management System (NBSLIMS)
- Bureau of Laboratories Laboratory Information Management System (BOLLIMS)
- Vital Event Registration Application (VERA)

According to the State of Michigan Financial Management Guide, MDHHS has primary responsibility for establishing, maintaining, and monitoring internal control* over its critical IT applications.

State of Michigan (SOM) technical standards indicate the Department of Technology, Management, and Budget (DTMB) is responsible for certifying compliance with established IT security policies, standards, and procedures.

Agency Services, within DTMB, has primary responsibility for designing, implementing, and executing IT general controls*. DTMB also develops, tests, and implements departments' IT applications and associated IT common and technical application controls* which incorporate the departments' business requirements. DTMB's Cyber Security division is responsible for the management of MILogin, the State's identification, credential, and access management system. MDSS and VERA use MILogin for system access.

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

AUDIT OBJECTIVE	To assess the sufficiency of MDHHS's and DTMB's security and user access controls over selected community health-related IT systems.
CONCLUSION	Not sufficient for MDHHS. Sufficient, with exceptions, for DTMB.
FACTORS IMPACTING CONCLUSION	• Two material conditions* related to a potential security breach and system security and access controls (Findings 1 and 2). • No reportable conditions* were identified related to read-only access roles for the four systems. • DTMB implemented security configurations for MILogin worker and third-party portals in accordance with SOM technical standards.

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

FINDING 1

Sensitive data potentially exposed to data breach.

MDHHS, in conjunction with DTMB, did not ensure appropriate security controls were in place over VERA's Internet Web site access point. As a result, sensitive data was potentially exposed to a data breach.

The State of Michigan Financial Management Guide (Chapter 1, Section 900) states departments have primary responsibility for establishing, maintaining, and monitoring internal control over their critical IT applications. Also, SOM Technical Standard 1340.00 states security controls must be implemented to protect SOM information from unauthorized access, use, disclosure, modification, destruction, or denial and to ensure confidentiality, integrity, and availability of SOM information. SOM Technical Standard 1340.00.020.03 indicates DTMB is responsible for certifying compliance with established IT security policies, standards, and procedures.

Improvements needed in security and access controls to sensitive data.

MDHHS utilized MILogin, which is SOM's centralized identity management solution, for VERA. However, because of concerns regarding the availability of MILogin, MDHHS created a process for system administrators to access VERA using a public facing Internet log-in page.

Our review disclosed:

- All users with active VERA accounts had the ability to log in to VERA using the Internet Web site.
- Significant security and access deficiencies which would not prevent or detect an unauthorized individual from accessing the system. Because of confidentiality concerns, we summarized our testing results for presentation in this finding and provided the underlying details to MDHHS and DTMB management.

After bringing these matters to management's attention, MDHHS locked down the access point into VERA. However, because of the lack of monitoring and identified control deficiencies, it would be extremely difficult to determine if a data breach had occurred.

MDHHS informed us it did not disable the Internet access to ensure access was available in the event MILogin experienced significant downtime.

We consider this finding to be a material condition because of the lack of significant security controls, which if in place would prevent and/or detect a potential breach of sensitive data.

RECOMMENDATION

We recommend that MDHHS, in conjunction with DTMB, ensure appropriate security controls are implemented for VERA's Internet Web site access point.

AGENCY PRELIMINARY RESPONSE

MDHHS and DTMB provided us with the following response:

MDHHS agrees with the recommendation and has disabled the access point. However, MDHHS does not believe that allowing access for 4 system administrators provided a significant risk of a potential data breach.

The internet site login path was secured, password protected, and set to lock after multiple incorrect login attempts. Passwords were only provisioned for system administrators and MDHHS only provided the login credentials to system administrators.

AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE*

VERA contains confidential health and personal data related to all births in Michigan. We consider "backdoor" access for systems containing confidential data to be a significant risk, especially when the access circumvents the State's MiLogin controls. Although MDHHS indicated it only provided credentials to system administrators, any user with login credentials could have found and made use of the backdoor access. Also, MDHHS and DTMB were not monitoring the backdoor access point and would not have identified if an unauthorized user logged into the system or if the data was breached. Upon bringing our concerns regarding the lack of security controls and monitoring to MDHHS's and DTMB's attention, the VERA Web site access point was promptly shut down. During a meeting on October 25, 2022, DTMB indicated this backdoor access point was not an approved solution and there was no business justification or need for this option to exist. Therefore, the finding stands as written.

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

FINDING 2

Access controls not fully established and implemented.

MDHHS, in conjunction with DTMB, did not fully establish and implement access controls over selected community health-related IT systems, which could lead to unauthorized access, disclosure, modification, or destruction of personally identifiable information.

SOM Technical Standard 1340.00.20.01 requires approval by an authorized requestor to create, modify, or delete information system accounts. Also, the Standard states access should be based on the principle of least privilege*. SOM Technical Standard 1340.00.020.03 affirms the agency is responsible for maintaining documentation of authorized users from the initial request to the de-registration of users who no longer require access to SOM protected IT resources. This Standard also affirms DTMB is responsible for certifying compliance with established IT security policies, standards, and procedures.

Improvements in procedures needed.

MDHHS, in conjunction with DTMB, did not:

a. Identify incompatible roles or excessive access rights to ensure effective segregation of duties* and access based on the principle of least privilege. We noted:

   (1) MDSS and VERA access forms did not require users to list the level of access they were requesting. Also, MDHHS did not maintain sufficient documentation to support incompatible roles were assessed for MDSS and VERA.

   (2) NBSLIMS and BOLLIMS users would list a similar user to have their access granted rather than requesting access rights based on their job responsibilities. Also, MDHHS did not maintain sufficient documentation to support incompatible roles were assessed for NBSLIMS and BOLLIMS. Identifying the specific permissions required for each user reduces the risk the permissions granted are beyond what is needed for the user's job function.

   Identifying incompatible roles is a key control in effective segregation of duties. Conversely, inadequate segregation of duties increases the risk erroneous or fraudulent transactions could be processed. MDHHS should limit access rights to those necessary users who perform day-to-day tasks to reduce the potential of inappropriate use of its applications.

b. Fully establish semiannual and annual recertifications. We noted:

   (1) MDHHS did not perform recertifications for MDSS during the audit period.

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

(2) MDHHS performed recertifications for NBSLIMS, BOLLIMS, and VERA but did not review users' roles/permissions to ensure the roles and permissions were still appropriate.

User access rights should be periodically recertified to ensure privileges granted to each user are still appropriate for the user's job responsibilities.

c. Ensure security configurations were appropriate for all four systems. Because of the confidentiality of these configurations, we summarized our testing results for presentation in this finding and provided the underlying details to MDHHS and DTMB management.

d. Fully implement effective internal control over the selected systems. We noted:

(1) All four systems did not have an effective process to grant access. This could lead to users receiving access in excess of what is required for their job functions.

(2) All four systems did not have an effective process to remove user access. Delayed removal can result in unauthorized access, potentially allowing users the ability to view, change, or update confidential information.

MDHHS informed us competing priorities and directives during the public health emergency, funding constraints, and insufficient training contributed to the internal control deficiencies. Also, DTMB did not sufficiently monitor MDHHS's adherence to SOM technical standards.

We consider this finding to be a material condition because of the numerous deficiencies identified related to security configurations and access management in relation to granting, removing, and recertifying users.

RECOMMENDATION

We recommend that MDHHS and DTMB fully establish and implement application access controls over the selected community health-related IT systems.

AGENCY PRELIMINARY RESPONSE

MDHHS and DTMB partially agree and provided us with their preliminary response. The response and our auditor's comments

providing further clarification on context where necessary are as follows:

AGENCY PRELIMINARY RESPONSE	AUDITOR'S COMMENTS TO AGENCY PRELIMINARY RESPONSE
a. *MDHHS agrees that there are opportunities for improvement to its processes used to identify incompatible roles for the MDSS, NBSLIM, and BOLLIM applications, however MDHHS does not agree with all components of the finding.*	
MDHHS agrees there is no system-generated list available, however, MDSS access is role driven and each role is designed to only allow the permissions needed for specific components of the application. MDHHS will modify the MDSS access application to require that users provide their current job responsibilities. All current State of Michigan users with access are being surveyed to assure that employment roles warrant assigned access. MDSS application administrators will document their role determination based on the user's job responsibilities.	MDSS's application form requires an individual to document their user type such as MDHHS staff, healthcare provider, laboratory, place of employment, and position title. However, the form does not list any of the roles within the MDSS system nor does it require an individual to identify the specific roles for which they are requesting access. During the audit, we requested a listing of user roles along with the purpose of the role and its capabilities. MDHHS was unable to provide a comprehensive listing for all current roles available within the system. Without a listing of user roles and their associated capabilities, MDHHS cannot ensure that incompatible role combinations have been identified.
MDHHS agrees that users were not required to list the level of access they were requesting, because access is governed by the user's place of employment, which is a required field on all access forms. For example, the birth certifier role is always granted to hospital and birthing center users and provides those users access to submit birth record information while the local registrar role is always granted to county and city clerk users and provides those users access to file birth records. Each role is designed to only allow the permissions needed for users at each place of employment. If a person were to work at multiple locations, their access only allows them to enter data in VERA at their primary assigned location. The assessment of incompatible roles is inherent as each user only has one place of employment.	VERA's application form does not contain a listing of roles within the system for an individual to choose from. The form contains areas for an individual to document their job title, description of job responsibilities, and work location. When we requested documentation to support MDHHS assessed incompatible roles, MDHHS indicated a formal assessment was unnecessary because it is their assertion a user can only be assigned to one location and the location governs the user's role within the system. However, MDHHS did not provide us with any documentation which crosswalks a user's work location to a role within the system. MDHHS's VERA User Guide contradicts their assertion users can enter data only into VERA at their primary assigned location. The VERA User Guide page 27 states: > Some users may have access to records in more than one office or location. For example, a midwife may deliver babies at several facilities. In this case, the midwife would have one login, but would have access to multiple offices using that login. By selecting the Change Office link from the Main Menu the midwife can quit working on cases in one hospital and begin working on cases in the other. VERA access should be granted based on a user's responsibilities and the principle of least privilege, rather than solely on the user's work location.
MDHHS will continue to evaluate potential system enhancements and solutions internally and seek input from the vendor if needed for NBSLIMS. MDHHS anticipates the NBSLIM application will be replaced by 2025. *MDHHS will enhance the access authorization process for BOLLIMS to ensure the privileges associated with each role are known to the requestor.*	

b. *MDHHS agrees that semi-annual and annual recertifications were not fully established for NBSLIMS, BOLLIMS, and VERA, however MDHHS disagrees that semi-annual and annual recertifications were not fully established for MDSS.*

MDHHS has an established recertification process in place for MDSS but paused that process due to competing priorities and directives throughout the Public Health Emergency. The recertification process was re-instated October 2022.

MDHHS is evaluating enhancements to the role selection and annual review processes for NBSLIM and BOLLIMS to ensure the appropriateness of user access rights are periodically recertified. MDHHS anticipates the NBSLIM application will be replaced by 2025.

MDHHS will also continue to evaluate both the feasibility of implementing the Database Security Application (DSA) and alternate solutions for VERA and MDSS application access.

Our review of users' last login date identified 1,183 accounts which should have been identified and inactivated during an annual recertification process due to inactivity. Although MDHHS indicated a pause was placed on recertifications during the public health emergency, 174 of the 1,183 accounts had last login dates of more than 60 days prior to the start of the public health emergency. Also, 23 accounts had last login dates as far back as 2017 but the accounts had not been disabled as of August 2022. If MDHHS's annual certification process was fully established and effective, then all accounts with a last login date 60 days prior to March 2020, the beginning of the public health emergency, would have been disabled within the system. Approximately 3,700 users should be reviewed annually and we noted annual reviews were skipped during 2020 and 2021.

c. *MDHHS will continue to evaluate both the feasibility of implementing the Database Security Application (DSA) and alternate solutions for VERA and MDSS application access. MDHHS will work internally and with the NBSLIMS and BOLLIMS vendors to evaluate potential system enhancements but anticipates the NBSLIM application will be replaced by 2025.*

d. *MDHHS does not agree that there was not an effective process to grant and remove user access for all applications.*

MDHHS has a process in place to lock inactive BOLLIMS accounts after 90 days of inactivity and retire them after 365 days of inactivity. MDHHS also has a Bureau of Laboratories (BOL) employee termination policy in place that applies to all BOL users who request access to NBSLIM or BOLLIMS. Users are only able to access NBSLIMS through State computers housed in the secure laboratory buildings and the termination process requires that an employee's access to the secure laboratory building is revoked on the day of their departure. The policy is required to be reviewed by all BOL employees annually.

BOLLIMS's and NBSLIMS's access request form does not document an individual's access within the system. The form documents the name of the individual's manager and the department/section/unit the individual works in and requires the individual to document the name of a similar user within their department/section/unit. The form does not require the individual to identify the role for which they are requesting access. For MDSS, MDHHS does not have documentation to demonstrate access was approved by an authorized requestor or the user's access is based on the principle of least privilege. In addition, MDHHS does not have a complete document demonstrating the access rights within MDSS and their capabilities.

Therefore, the department had not fully implemented effective control over system access.

MDHHS's process to lock inactive BOLLIMS accounts after 90 days of inactivity does not meet SOM Technical Standard 1340.00.020.01 which requires the account to be disabled after 60 days of inactivity. SOM Technical Standard 1340.00.020.01 also requires a user's access to be removed within 48 hours of termination or transfer. MDHHS did not have an approved exception to the SOM technical standards. During our review of user access, MDHHS identified 2 users which should have had their access removed. One user's access extended 60 days beyond their departure.

In addition, users are not able to access NBSLIMS without an active directory account, which is flagged after 60 days of inactivity and deleted after 90 days of inactivity. MDHHS anticipates the NBSLIM application will be replaced by 2025.

MDHHS will also update the process to lock inactive accounts after 60 days of inactivity for BOLLIMS and NBSLIMS.

MDHHS's process to lock inactive NBSLIMS's accounts after 90 days of inactivity does not meet SOM Technical Standard 1340.00.020.01 which requires the account to be disabled after 60 days of inactivity. MDHHS did not have an approved exception to not follow the SOM technical standard.

Although MDHHS is relying on Active Directory, it cannot be certain DTMB revoked or disabled access in a timely manner as noted in our July 2017 Statewide Windows Active Directory Environments performance audit report (071-0564-16). In addition, it is possible for a user to switch divisions or departments retaining their Active Directory account. If not removed from NBSLIMS, it could still be available in their single sign-on portal. Therefore, relying on Active Directory is not a valid control.

We were unable to fully test timely removal of access because NBSLIMS does not contain account deactivation/disable dates. However, during our review of user access, MDHHS identified 25 user accounts which should have had access removed.

MDHHS requires VERA application users to fill out an access form and complete required training. Two levels of approval are required prior to any user access authorization.

MDHHS will modify the MDSS access application to require that users provide their current job responsibilities. MDSS application administrators will document their role determination based on the user's job responsibilities. MDHHS will also implement automatic removal of MDSS user access after 60 days of inactivity and communicate the importance of notifying MDSS administrators of staff departures to applicable managers.

MDHHS will also continue to evaluate both the feasibility of implementing the Database Security Application (DSA) and alternate solutions for VERA and MDSS application access.

VERA users do not list a role they need access to; instead, they list their job function and a VERA system administrator assigns a role based on the job function. In addition, MDHHS does not have a crosswalk of which roles should be assigned to which job functions. Therefore, the department cannot determine if the users received the proper role, if the role met the principle of least privilege, or if there were segregation of duties issues (which could lead to incompatible roles being assigned).

We were unable to test timely removal of access because an individual's start and end dates in VERA are configurable and do not represent the actual date the user was added or removed from VERA.

Therefore, the department had not fully implemented effective controls over removal of user access for BOLLIMS, NBSLIMS, and VERA.

The finding stands as written.

SYSTEM DESCRIPTION

MDHHS utilizes IT systems for collecting and reporting community health-related information. MDHHS has more than 80 community health-related IT systems.

We conducted a risk assessment* and identified the following systems within our audit scope:

- MDSS
  MDHHS uses MDSS for electronic disease data capturing, case management and tracking, exposure monitoring and investigating, and contact tracing. MDSS can receive disease reports through manual entry, online Web submission of case referral/intake reports, or importation of electronic laboratory reports. MDSS shares information with the Centers for Disease Control and Prevention's (CDC's) National Notifiable Diseases Surveillance System. As of August 15, 2022, MDSS had 3,747 active user accounts including healthcare providers, laboratories, local health departments, and SOM workers.

- NBSLIMS
  NBSLIMS is used to track and process all blood samples through the laboratory from receipt to reporting results. The Newborn Screening Laboratory, a section of the Chemistry and Toxicology Division of MDHHS, screens all Michigan newborns for certain detectable life-threatening and/or disabling disorders. Test results are reported to the submitter of the sample and, when necessary, to a team of follow-up healthcare professionals who ensure any children having a disorder receive appropriate treatment. As of August 8, 2022, NBSLIMS had 116 active user accounts.

- BOLLIMS
  BOLLIMS is essential to the required functions of laboratory specimen processing and test reporting to the Infectious Disease Division and the Chemistry and Toxicology Division within the MDHHS's Bureau of Laboratories. These specimens are tracked, tested, and reported and the information is retained for epidemiological studies or submission to adjunct agencies and systems, such as the CDC and MDSS. As of September 1, 2022, BOLLIMS had 379 active user accounts.

- VERA
  MDHHS uses VERA to collect information for all births in Michigan and to generate birth certificates. MDHHS also uses VERA to collect statistical data to identify birth defect

** See glossary at end of report for definition*

trends. Data collected and stored in VERA is extracted and sent to various MDHHS systems. VERA was implemented May 1, 2020, and as of August 2022, VERA had approximately 800 active user accounts composed of SOM, hospital, local health department, and county health department workers.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine MDSS, NBSLIMS, BOLLIMS, and VERA records related to security and access controls over the systems. 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.

As part of the audit, we considered the five components of internal control (control environment, risk assessment, control activities, information and communication, and monitoring activities) relative to the audit objectives and determined all components were significant.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2021 through September 30, 2022.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of MDHHS's and DTMB's security and user access controls for the selected community health-related IT systems to establish our audit objective, scope, and methodology. During our preliminary survey, we:

- Obtained an understanding of the selected community health-related IT systems.
- Interviewed MDHHS management and staff responsible for administering and securing MDSS, NBSLIMS, BOLLIMS, and VERA.
- Interviewed DTMB management and staff responsible for administering and securing MILogin as it pertains to MDSS and VERA.
- Reviewed SOM policies and procedures related to MDSS, NBSLIMS, BOLLIMS, and VERA security and access controls.
- Reviewed system documentation, including the contracts, for MDSS, NBSLIMS, BOLLIMS, and VERA development, implementation methodology, and system configurations.

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

- Obtained an understanding of MDHHS's and DTMB's key processes, systems, and internal control significant to the potential audit objectives.

- Obtained an understanding of MDHHS's and DTMB's processes for:

    - Granting, monitoring, and removing user access to MDSS, NBSLIMS, BOLLIMS, and VERA.

    - Monitoring privileged user access.

OBJECTIVE

To assess the sufficiency of MDHHS's and DTMB's security and user access controls over selected community health-related IT systems.

To accomplish this objective for MDSS, NBSLIMS, BOLLIMS, and VERA, we:

- Interviewed MDHHS's management and staff to obtain an understanding of the security and access controls implemented.

- Judgmentally selected users with active accounts during October 1, 2021 through September 30, 2022 for each system to better understand, evaluate, and form conclusions on the design and implementation of MDHHS's internal control procedures against SOM policy and industry best practices for granting, removing, and recertifying access. This serves as the basis for our conclusions.

- Interviewed MDHHS management to obtain an understanding of segregation of duties.

- Judgmentally selected and tested security configurations against SOM policy and industry best practices.

For our judgmental selections, we could not project the results to the respective populations.

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.

CONFIDENTIAL AND SENSITIVE INFORMATION

Because of confidentiality concerns, we summarized our testing results for presentation in the report and provided the underlying details to MDHHS and DTMB management.

AGENCY RESPONSES

Our audit report contains 2 findings and 2 corresponding recommendations. MDHHS and DTMB's preliminary response indicates they agree with 1 recommendation and partially agree with 1 recommendation.

The agency preliminary response following each recommendation in our report was taken from the agencies' 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.
application controls	Controls that are directly related to individual computer applications. These controls help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.
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.
availability	Timely and reliable access to data and information systems.
BOLLIMS	Bureau of Laboratories Laboratory Information Management System.
CDC	Centers for Disease Control and Prevention.
confidentiality	Protection of data from unauthorized disclosure.
DTMB	Department of Technology, Management, and Budget.
general controls	The structure, policies, and procedures that apply to an entity's overall computer operations. These controls include an entitywide security program, access controls, application development and change controls, segregation of duties, system software controls, and service continuity controls.
integrity	Accuracy, completeness, and timeliness of data in an information system.
internal control	The organization, policies, and procedures adopted by management and other personnel to provide reasonable assurance that operations, including the use of resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations

	are followed. Internal control also includes the safeguarding of assets against unauthorized acquisition, use, or disposition.
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.
MDSS	Michigan Disease Surveillance System.
NBSLIMS	Newborn Screening Laboratory Information Management System.
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 charge 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 actions, and contribute to public accountability.
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 they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes.
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.
risk assessment	The process of identifying risks to entity operations (including mission, functions, image, or reputation), entity assets, or persons by determining the probability of occurrence, the resulting impact, and additional security controls that would

	mitigate this impact. Risk assessment is a part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
segregation of duties	Separation of the management or execution of certain duties or areas of responsibility to prevent or reduce opportunities for unauthorized modification or misuse of data or service.
SOM	State of Michigan.
VERA	Vital Event Registration Application.

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8070