Office of the Auditor General
Performance Audit Report

Driver and Vehicle Related Systems

Department of State and
Department of Technology, Management, and Budget

April 2015

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

231-0525-14

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.

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Performance Audit

Driver and Vehicle Related Systems

Department of State and Department of Technology, Management, and Budget

Report Number:
231-0525-14

Released:
April 2015

The Department of State (DOS) uses various information systems to manage and process its driver and vehicle related transactions. The Department of Technology, Management, and Budget (DTMB) provides information technology support services for these systems. During fiscal year 2013, DOS collected $2.2 billion in taxes and fees from driver's licenses and vehicle registrations and titles.

Audit Objective	Conclusion
Objective #1: To assess the effectiveness of DOS and DTMB's efforts to ensure the timely, accurate, and complete processing of selected driver and vehicle related data by the Unisys mainframe.	Moderately effective

Finding Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DOS should strengthen its controls over the updating of external data to driver and vehicle records on the mainframe to help ensure timely, accurate, and complete updates of conviction and stolen vehicle data (Finding #1).		X	Partially agrees

Audit Objective	Conclusion
Objective #2: To assess the effectiveness of DOS and DTMB's efforts to implement security and access controls over selected driver and vehicle related systems.	Moderately effective

Findings Related to This Audit Objective	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB did not fully establish security and access controls over key databases that DOS uses to process driver and vehicle related transactions, increasing the risk of confidential data loss and unauthorized access to confidential data (Finding #2).		X	Agrees

Findings Related to This Audit Objective (*Continued*)	Material Condition	Reportable Condition	Agency Preliminary Response
DTMB did not establish effective security and access controls over key operating systems, which increases the risk of unauthorized access to confidential data (Finding #3).		X	Agrees
DOS did not fully implement effective access controls over key driver and vehicle related systems to prevent selected users from viewing or accessing records that they are not authorized to view or access (Finding #4).		X	Agrees

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: http://audgen.michigan.gov

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
201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • http://audgen.michigan.gov

Doug A. Ringler, CPA, CIA
Auditor General

April 14, 2015

The Honorable Ruth Johnson
Secretary of State
Richard H. Austin Building
Lansing, Michigan
and
Mr. David B. Behen
Director, Department of Technology, Management, and Budget
Chief Information Officer, State of Michigan
Lewis Cass Building
Lansing, Michigan

Dear Secretary Johnson and Mr. Behen:

I am pleased to provide this performance audit report on Driver and Vehicle Related Systems, Department of State and Department of Technology, Management, and Budget.

We organized the background, findings, and recommendations by audit objective. 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 submit it within 60 days of the date above to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services 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

DRIVER AND VEHICLE RELATED SYSTEMS

This Page Left Intentionally Blank

BACKGROUND, FINDINGS, AND RECOMMENDATIONS

ENSURING TIMELY, ACCURATE, AND COMPLETE PROCESSING OF DATA

AUDIT OBJECTIVE	To assess the effectiveness* of the Department of State (DOS) and the Department of Technology, Management, and Budget's (DTMB's) efforts to ensure the timely, accurate, and complete processing of selected driver and vehicle related data by the Unisys mainframe.
CONCLUSION	Moderately effective.
FACTORS IMPACTING CONCLUSION	• No material conditions* related to processing controls. • Moderate, but not severe, impact of the reportable condition* (Finding #1) on DOS's ability to effectively process driver and vehicle related data.

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

FINDING #1

Strengthened controls over the updating of external data would help ensure timely, accurate, and complete updates.

DOS should strengthen its controls over the updating of external data to driver and vehicle records on the mainframe to help ensure timely, accurate, and complete updates of conviction and stolen vehicle data.

Control Objectives for Information and Related Technology* (COBIT) states that input errors should be identified and corrected in a timely and appropriate manner.

DOS receives electronic data from external entities to update driver and vehicle records. This data includes driver conviction records, vehicles reported as stolen, and deceased individuals. Generally, when DOS electronically processes the data, driver and vehicle records in the mainframe are appropriately updated. However, for some records, data irregularities may result in errors and cause the mainframe to not properly update the records. An error report is produced that contains the reasons why the records were not electronically updated. Manual intervention is then required by DOS or the external entity that sent the data to ensure that the records are properly updated.

Our review of the process to update driver and vehicle records with external data disclosed that DOS did not perform an effective review and reconciliation of:

a. Driver conviction data for the 17,671 errors that occurred from June 2013 through May 2014.

   When errors occur in the electronic processing of conviction data, the court of law where the record originated should correct and resubmit the data to DOS. DOS implemented a process to review a sample of the errors to ensure that the errors were corrected by the courts and that the driver records were subsequently updated. However, the sample included only 184 (1%) of the 17,671 errors from June 2013 through May 2014. In addition, DOS did not consistently document whether the 184 sampled records had been corrected and updated on the driver records. Most of the 17,671 errors had been subsequently corrected and added to the driver records. However, we could not locate 2,630 (15%) of the 17,671 errors in the driver records for the license numbers sent by the courts.

   Although some of the 2,630 errors may have been properly updated under other license numbers or may be acceptable because of other reasons, DOS cannot ensure that the driver records are accurate for the 2,630 errors unless DOS strengthens its reconciliation controls.

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

b. Stolen vehicle data for the 2,709 stolen vehicle records with errors from June 2013 through May 2014.

   DOS indicated that the Michigan Department of State Police (MSP) normally resubmits the data to the mainframe after MSP has corrected the errors. However, DOS had not implemented a process to verify that the errors had actually been corrected. Because stolen vehicle data plays an integral role in ensuring appropriate mainframe processing, DOS should improve its process to verify that the error records are updated in a timely and accurate manner.

RECOMMENDATION

We recommend that DOS strengthen its controls over the updating of external data to driver and vehicle records on the mainframe to help ensure timely, accurate, and complete updates of conviction and stolen vehicle data.

AGENCY PRELIMINARY RESPONSE

DOS provided us with the following response:

DOS partially agrees. It is DOS's position that court input errors ultimately must be corrected by the court and resubmitted to DOS properly and correctly in accordance with State law [*Section 257.732(3) of the* Michigan Compiled Laws]*. DOS is unable to record an incorrect or improperly prepared abstract to a driving record* [*Section 257.320a(1) of the* Michigan Compiled Laws]*. However, the DOS/court partnership will continue its error mitigating efforts and enhance those efforts by:*

- *Doubling the sample size of the courts currently included in the review process.*
- *Tracking errors found in the samples to ensure that they have been corrected and resubmitted to DOS by the court.*
- *Following up with the court to determine disposition if the abstract is not found to be corrected within 60 days.*
- *Providing error data to DOS court liaisons for follow-up with the court if the error is not corrected within 60 days.*
- *Determining the feasibility of resolving errors programmatically.*
- *Providing a quarterly error report to assist courts with error resolution.*

DOS believes that these additional actions will help further ensure that timely, accurate, and complete updates of abstract data are properly posted to driving records and will address the concerns noted in the audit.

DOS concurs with the audit finding in that DOS did not perform an effective review and reconciliation of stolen vehicle interface errors. The vast majority of stolen vehicle reports submitted via the Law Enforcement Information Network (LEIN) to DOS appear seamlessly on DOS records without interruption. Of the stolen vehicle submissions that do not appear on DOS records, many are the result of input errors in LEIN.

DOS recognizes the importance of ensuring the accuracy and integrity of its records and will promptly initiate a review and reconciliation in partnership with MSP to process stolen vehicle interface errors to further enhance the timeliness, accuracy, and completeness of its records.

IMPLEMENTING SECURITY AND ACCESS CONTROLS OVER SELECTED DRIVER AND VEHICLE RELATED SYSTEMS

BACKGROUND

Security* and access controls* limit or detect inappropriate access, which is important to ensure the availability*, confidentiality*, and integrity* of data.

AUDIT OBJECTIVE

To assess the effectiveness of DOS and DTMB's efforts to implement security and access controls over selected driver and vehicle related systems.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- Potential impact that the reportable conditions (Findings #2 through #4) could have on system security.
- Criticality of data stored in the systems.

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

FINDING #2

More comprehensive security and access controls are vital to protecting key DOS databases.

DTMB did not fully establish security and access controls over key databases that DOS uses to process driver and vehicle related transactions, increasing the risk of confidential data loss and unauthorized access to confidential data.

The Federal Information System Controls Audit Manual* (FISCAM) states that security settings should be configured to the most restrictive mode consistent with operational requirements. FISCAM also states that user access should be limited to individuals with a valid business purpose and access authorization forms should be maintained. In addition, DTMB Technical Standard 1340.00.15 states that automated log management should be used to monitor the activity of privileged users.

Our review of security and access controls over the Accounts Receivable System (ARS), Business Application Modernization (BAM), and Computerized OnLine Data (COLD) databases disclosed that DTMB did not:

a. Effectively monitor the third party contractors' security configurations of the ARS, BAM, and COLD databases.

   DTMB contracts with third parties to manage the security configurations of the ARS, BAM, and COLD databases. DTMB was not cognizant of the benchmarks used by third party contractors to secure the databases and the current security configurations of the databases. Failure to effectively monitor the database security configurations increases the risk of confidential data loss and unauthorized access to the confidential data.

b. Ensure the effective configuration of ARS, BAM, and COLD database security settings, such as profile settings and configuration parameters.

   Configuration of database security settings not in compliance with best practices.

   We reviewed 64 security settings for ARS, 31 security settings for BAM, and 32 security settings for COLD and noted that 15, 9, and 8 security settings, respectively, were not in compliance with best practices. Proper configuration of the database security settings reduces the risk of loss of or unauthorized access to confidential data.

c. Sufficiently restrict access to the ARS and BAM databases.

   Fifteen ARS user accounts were no longer used, and 1 user account had an invalid user name. Also, 2 BAM user accounts belonged to users who were no longer on the BAM Project, 3 BAM user accounts were no

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

longer being used, and 1 test user account had access to the production database. As a result, users who did not have a valid business need had access to the production databases.

d. Document and maintain the authorization and approval of user access to DOS databases.

   We requested access authorization forms for 17 ARS, BAM, and COLD database users and noted that 16 of the users did not have documented authorization for database access. Documenting authorization and approval of database access helps to ensure that only appropriate individuals have access to the database and that privileges assigned to them are appropriate.

e. Use database audit logs to monitor the activity of the ARS, BAM, and COLD database administrators* (DBAs) and other privileged accounts.

   Audit logs maintain privileged access* information, which can help identify unusual or unauthorized activity. Recording and monitoring selected high-risk actions by the DBAs would help enhance database security.

RECOMMENDATION

We recommend that DTMB fully establish security and access controls over key databases that DOS uses to process driver and vehicle related transactions.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and will fully establish security and access controls. DTMB will enforce the existing Database Security Standard (1340.00.15) in all agency databases. Also, DTMB's Database Security Program Office will maintain records of controls being properly managed on all database security standards. In addition, DTMB will ensure that internal reviews occur frequently and randomly on each agency's databases to ensure compliance. The Database Security Program Office will assign a DBA security specialist to work with each agency to assist in training DBAs on how to properly secure their databases following the 1340.00.15 standard and other best practices available.

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

FINDING #3

Improvements are needed to operating system access controls.

DTMB did not establish effective security and access controls over key operating systems*, which increases the risk of unauthorized access to confidential data.

A well-secured operating system helps provide a stable environment on which to run DOS's information systems. DTMB Administrative Guide policy 1340 requires the secure establishment, maintenance, and administration of servers, including operating system software and the data residing on the servers. In addition, COBIT states that servers should be secured at a level equal to or greater than the defined security requirements of the information being processed, stored, or transmitted.

Our review of operating system security disclosed that DTMB did not:

Security configurations inconsistent with industry best practices.

a. Review operating system configurations to ensure that configuration settings were consistent with industry best practices.

   Each of 36 servers for ARS, BAM, and COLD had vulnerable* operating system configurations. Because of the confidentiality of operating system configurations, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to DTMB management.

b. Establish effective segregation of duties* between operating system administrators* and DBAs.

   Three BAM DBAs and one COLD DBA had administrative access to the operating system. Best practices state that database access rights should be limited to the DBA team and that management of the operating system should be limited to the operating system administration team.

c. Document and maintain the authorization and approval of operating system access for ARS, BAM, and COLD users.

   Such approval would help ensure that only appropriate individuals have access to the operating system and that privileges assigned are appropriate.

d. Have an effective process to review access to the operating systems and disable user accounts for users who no longer required access.

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

Two users in COLD, including one operating system administrator, were no longer employed by the State but still had system access.

RECOMMENDATION

We recommend that DTMB establish effective security and access controls over key operating systems.

AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation and will continue its efforts to establish effective security and access controls over key operating systems. DTMB is in the process of implementing an automated configuration management tool that will assist in rapidly deploying, maintaining, and auditing operating system security and access controls. The automated configuration management tool will also assist in monitoring changes from the required minimal service configurations and deviations from the approved operating system configuration settings. The result will be used by the server team to keep or bring the operating system back into compliance.

FINDING #4

Improvements are needed to driver and vehicle related system access controls.

DOS did not fully implement effective access controls over key driver and vehicle related systems to prevent selected users from viewing or accessing records that they are not authorized to view or access.

FISCAM states that access controls should be implemented at the system level to provide reasonable assurance that only authorized personnel have access to the system and only for authorized purposes. FISCAM also states that access should be limited to individuals with a valid business purpose.

Our review of the BAM, COLD, and Screen Machine applications disclosed that DOS:

Crosswalk of high-risk functionality and user roles not developed.

a. Had not developed a framework to crosswalk the high-risk functionality in BAM to the user roles that have the ability to perform the high-risk functionality.

   During BAM development, DOS created a matrix of BAM functionality and the user roles allowed to perform the functionality. However, DOS did not document which of the functionalities within the matrix are high-risk functions. Functionality may be considered high risk because it allows a user to perform certain types of transactions or to view confidential information. Identifying and documenting high-risk functionality is important to ensure effective monitoring and restriction of user activity and identification of incompatible roles.

Approval of user access not documented.

b. Did not document and maintain the authorization and approval of application access for COLD and Screen Machine users.

   Of 50 COLD users and 13 Screen Machine users reviewed, 40 and 12 users, respectively, did not have documented authorization. Authorization of access is important to ensure that privileges are assigned consistent with the users' job responsibilities and that DOS is aware of users with access to sensitive data.

c. Did not periodically review users' access to BAM, COLD, and Screen Machine or have a practical method for obtaining a listing of BAM users and their associated privileges to assist management in performing periodic reviews.

   DOS had not reviewed BAM access since April 2013. Three (10%) of 30 BAM users selected, 5 (10%) of 50 COLD users selected, and 1 (8%) of 13 Screen Machine users selected no longer had appropriate access and should have been removed.

RECOMMENDATION

We recommend that DOS fully implement effective access controls over key driver and vehicle related systems.

AGENCY PRELIMINARY RESPONSE

DOS provided us with the following response:

DOS agrees and will continue to work to implement improvements to application access controls over its driver and vehicle related systems, including BAM, COLD, and Screen Machine. These efforts will include further refinements to the overall information security strategy deployed for BAM, including application access controls based on a recently completed information security review. Also, DOS will implement new procedures to have all program areas complete annual user reviews to update access documentation and ensure that users no longer have system access beyond their current needs.

AGENCY AND SYSTEM DESCRIPTION

DOS has stated its commitment to delivering modern, efficient, cost-effective, and convenient service achieved with innovation and technology. DOS is responsible for licensing drivers and registering and titling vehicles. DOS uses the following information systems to manage and process its driver and vehicle related transactions:

- The Accounts Receivable System (ARS) is an automated accounting system used to create invoices, process revenue transactions, and approve refund transactions related to driver and vehicle activity.

- Business Application Modernization (BAM) is a client-server system that was developed to modernize and improve DOS business processes and replace the legacy information systems that support DOS business operations, including driver licensing, identification card issuance, vehicle titling, vehicle registration, and voter registration. The Web portion of BAM, called ExpressSOS, provides Michigan residents with the ability to process certain transactions on-line. At the time of our audit, BAM was still under development.

- The Branch Office System is an automated system used at Secretary of State branch offices to process driver and vehicle related transactions. It will be replaced by BAM when BAM is fully implemented.

- Computerized OnLine Data (COLD) is an automated system that receives data from the mainframe and converts it into various reports. COLD generates numerous reports related to driver and vehicle information.

- Renewal By Mail is an automated system that reads and batches driver and vehicle related transactions submitted via mail and submits the information to the mainframe for processing.

- Screen Machine is an on-line data entry system that allows a user to create and modify mainframe driver and vehicle related data as needed.

- Self-service stations, also known as kiosks, are ATM-style machines located in branch offices. Self-service stations can be used by customers to renew their vehicle tabs.

- The Unisys mainframe processes the majority of all driver and vehicle related transactions. A mainframe database contains the master driver and vehicle records for the State of Michigan.

During fiscal year 2013, DOS collected $2.2 billion in taxes and fees from driver's licenses and vehicle registrations and titles, including $1.0 billion in sales and use taxes on motor vehicles and $1.0 billion in motor vehicle title and registration fees.

DTMB Technical Services is responsible for maintaining, supporting, and securing the servers upon which ARS, BAM, and COLD are stored and processed.

DTMB Agency Services is responsible for providing software development and delivering and coordinating information technology* services. Agency Services also administers the databases for ARS and COLD.

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

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

Our audit scope was to examine the information processing and other records of driver and vehicle related 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.

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered the period June 1, 2013 through May 31, 2014.

METHODOLOGY

We conducted a preliminary survey of selected driver and vehicle related systems to formulate a basis for defining the audit objectives, scope, and methodology. During our preliminary survey, we:

- Interviewed DTMB and DOS staff and reviewed system documentation to obtain an understanding of the various driver and vehicle related programs.
- Obtained an understanding of the various information systems used by DOS to process driver's license and vehicle registration and title transactions.
- Attended a demonstration of ARS, COLD, and the mainframe job scheduler and processor, known as BLSched, to obtain an understanding of each system and how they are utilized by DOS in the driver's license and vehicle registration and titling processes.

OBJECTIVE #1

To assess the effectiveness of DOS and DTMB's efforts to ensure the timely, accurate, and complete processing of selected driver and vehicle related data by the Unisys mainframe.

To accomplish our first objective, we:

- Judgmentally selected various interfaces and assessed the timeliness, accuracy, and completeness of processing of the interfaces by the mainframe to determine if data was appropriately updated to driver and vehicle records.
- Judgmentally selected data processing jobs performed by the mainframe to determine if all driver and vehicle records were appropriately updated.

- Obtained information from MSP to substantiate our testing of the data interface of stolen vehicle records.

- Reviewed various datasets to ensure that the data stored on the mainframe was valid.

- Judgmentally selected portions of the *Michigan Compiled Laws* to verify that the driver and vehicle records in the datasets were in compliance.

OBJECTIVE #2

To assess the effectiveness of DOS and DTMB's efforts to implement security and access controls over selected driver and vehicle related systems.

To accomplish our second objective, we:

- Interviewed DOS and DTMB staff and reviewed DTMB policies and procedures to obtain an understanding of the security and access controls over the ARS, BAM, COLD, and Screen Machine applications.

- Reviewed controls over the ARS, BAM, and COLD databases and operating systems.

- Reviewed the service level agreement between DOS and DTMB and the third party vendor contracts with the State to obtain an understanding of each party's roles and responsibilities for security of the systems.

- Judgmentally selected and evaluated configuration settings of the databases and operating systems for appropriateness with industry standards and best practices.

- Judgmentally selected and evaluated the access rights of user accounts that had access to the applications, databases, and operating systems for appropriateness with job roles and responsibilities.

CONCLUSIONS

We based our conclusions on our audit efforts as described in the preceding paragraphs and the resulting reportable conditions noted in the background, findings, and recommendations section. The reportable conditions are less severe than a material condition but represent opportunities for improvement and deficiencies in internal control*.

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

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. DOS and DTMB's preliminary response indicates that they agree with 3 and partially agree with 1 of the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the agencies' written comments and oral discussion at the end of our audit 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 submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services 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.
ARS	Accounts Receivable System.
ATM	automated teller machine.
availability	Timely and reliable access to data and information systems.
BAM	Business Application Modernization.
COLD	Computerized OnLine Data.
confidentiality	Protection of data from unauthorized disclosure.
configuration	The way a system is set up. Configuration can refer to either hardware or software or the combination of both.
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 information technology.
database	A collection of information that is organized so that it can be easily accessed, managed, and updated.
database administrator (DBA)	The person responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users of the database. Additional responsibilities include operation, performance, integrity, and security of the database.
DOS	Department of State.
DTMB	Department of Technology, Management, and Budget.

effectiveness	Success in achieving mission and goals.
Federal Information System Controls Audit Manual (FISCAM)	A methodology published by the U.S. Government Accountability Office (GAO) for performing information system control audits of federal and other governmental entities in accordance with *Government Auditing Standards.*
information technology	Anything related to computing technology, such as networking, hardware, software, the Internet, or the people who work with these technologies.
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.
LEIN	Law Enforcement Information Network.
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.
MSP	Michigan Department of State Police.
operating system	The essential program in a computer that manages all the other programs and maintains disk files, runs applications, and handles devices such as the mouse and printer.
operating system administrator	The person responsible for administering use of a multiuser computer system, a communications system, or both.

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.
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.
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.
vulnerability	Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank


OAG
Office of the Auditor General
Independent
Objective
Transparent