Office of the Auditor General
Performance Audit Report

Office of Investigative Services Enforcement Division

Department of State

May 2021

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

231-0234-20

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
Office of Investigative Services Enforcement Division
Department of State

Report Number:
231-0234-20

Released:
May 2021

The Office of Investigative Services Enforcement Division's mission is to detect, reduce, and deter fraud in the Department of State programs, as well as assist in providing a safe and secure work environment for Department personnel and facilities. This mission is carried out through a network of branch examinations, investigations, data analysis, and investigative and security support functions. For fiscal year 2019, the Division expended $3.0 million. As of May 31, 2020, the Division had 32 full-time employees.

Audit Objective			Conclusion
Objective #1: To assess the sufficiency of the Division's efforts to deter, detect, and investigate potential fraud.			Sufficient, with exceptions
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
An increased risk of uninsured drivers existed because the Insurance Fraud Prevention Unit had not reviewed over 46,000 cases for potentially fraudulent insurance policies (Finding #1).		X	Agrees

Audit Objective			Conclusion
Objective #2: To assess the effectiveness of the Division's efforts to ensure the completeness and accuracy of its case management system.			Moderately effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
Improvements in security over the case management system are needed to help ensure that sensitive investigation details are protected from unauthorized access, modification, and disclosure (Finding #2).		X	Agrees

Audit Objective			Conclusion
Objective #3: To assess the sufficiency of the Division's efforts to help ensure safety and security at branch offices.			Sufficient, with exceptions
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
We identified 44 former or inactive employees and contractors with the access codes to gain entry into branch offices. One individual had not been employed by the Department for over 10 years (Finding #3).		X	Agrees
Improvement in the documentation and resolution of surveillance system equipment issues is needed to ensure resolution of equipment issues and limit surveillance interruptions (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

May 25, 2021

The Honorable Jocelyn Benson
Secretary of State
Richard H. Austin Building
Lansing, Michigan

Dear Secretary Benson:

This is our performance audit report on the Office of Investigative Services Enforcement Division, Department of State.

We organize our findings and observations 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 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

OFFICE OF INVESTIGATIVE SERVICES ENFORCEMENT DIVISION

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

DETERRENCE, DETECTION, AND INVESTIGATION OF POTENTIAL FRAUD

BACKGROUND

The Office of Investigative Services Enforcement Division completes branch examinations and investigations and performs data analysis to help deter, detect, and investigate alleged fraud occurring within the Department of State programs. The Division conducts examinations of Secretary of State branch offices to assess performance and compliance with procedures and performs special examinations of branch personnel involved in fraud allegations or procedural violations.

The Division also investigates vehicle registration transactions in which the insurance policy information could not be verified through the Secretary of State's Electronic Insurance Verification (EIV) program. All auto insurers writing policies for Michigan residents are required to submit each policyholder's information using the EIV program, as described in Public Acts 91 and 92 of 2011. If the insurance cannot be verified through the EIV program, the case is referred to the Insurance Fraud Prevention Unit (IFPU).

AUDIT OBJECTIVE

To assess the sufficiency of the Division's efforts to deter, detect, and investigate potential fraud.

CONCLUSION

Sufficient, with exceptions.

FACTORS IMPACTING CONCLUSION

- The Division assigned or referred potential fraud allegations in a timely manner to its Fraud Investigations Section (FIS) for further investigation.
- The Division appropriately prioritized its review of branch offices to ensure that those offices with certain indicators were reviewed.
- The Division conducted and appropriately documented in a timely manner its standard and special branch office reviews and FIS investigations.
- The Customer and Automotive Records System* (CARS) access granted to Division employees was reasonable and appropriate based on the employees' assigned job functions.
- Reportable condition* related to improving the timeliness of IFPU's vehicle insurance reviews (Finding #1).

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

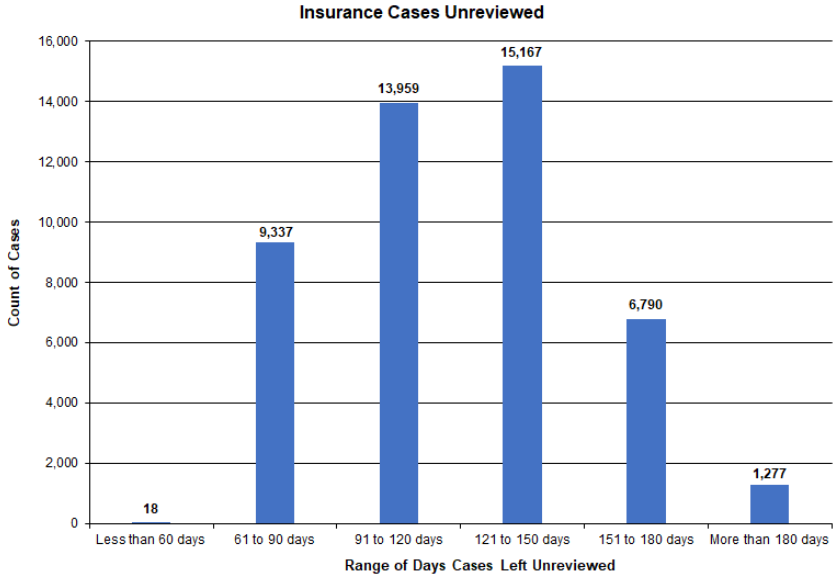
FINDING #1

Improvement needed in the timeliness of vehicle insurance reviews.

IFPU did not always timely review the insurance cases that could not be verified through the EIV program. This may have allowed fraudulent insurance policies to go undetected, increasing the possibility that uninsured vehicles are being operated on the roadway.

Section 500.3101 of the *Michigan Compiled Laws* requires that vehicles have insurance at the time of registration and when driven. Department of State policy requires that IFPU verify that a vehicle had valid insurance at the time of the registration or renewal for referred cases that could not be verified electronically.

We analyzed approximately 523,400 insurance cases that were referred through branch office transactions from February 18, 2019 through May 31, 2020 and identified 46,548 cases that IFPU had not yet reviewed as of August 27, 2020:



The Division informed us that limited resources contributed to the backlog of unreviewed cases and that there are several pending CARS enhancements that should improve efficiencies.

RECOMMENDATION

We recommend that IFPU timely review the insurance cases that could not be verified through the EIV program.

AGENCY PRELIMINARY RESPONSE

The Department provided us with the following response:

The Department agrees with the recommendation and will continue its efforts in reviewing insurance policies that cannot be verified through the Electronic Insurance Verification (EIV) process. The Department is working on enhancements to the Customer and Automotive Records System (CARS) that will assist in improving the efficiency of the IFPU's ability to identify fraudulent insurance policies. One of the enhancements was

implemented in November 2020, with additional enhancements to follow. In addition, the Department implemented a risk-based data analytics methodology in determining the insurance policies it will review. This will assist in the elimination of potentially fraudulent policies going undetected by focusing on known fraudulent indicators.

COMPLETENESS AND ACCURACY OF THE CASE MANAGEMENT SYSTEM

BACKGROUND

The Division's case management system utilizes a Microsoft Access database to record, track, and monitor allegations of fraud referred via the fraud tip hotline, phone, e-mail, branch offices, law enforcement, and other State or federal agencies. All allegations received are recorded in the case management system and receive a case number. If it is determined that the Division does not have the jurisdiction to open and investigate the case, it is referred to the applicable investigating entity and the case is closed. If the Division has jurisdiction to investigate, it assigns a FIS agent and findings are documented within the system. The Investigative Analytics Section (IAS) also uses the case management system to record requests for assistance from internal Department investigators, law enforcement, and other government agency investigators. The case management system includes information related to potential, active, and closed investigative cases and requests for assistance, such as victim, suspect, and witness interviews and contact information.

From October 1, 2017 through May 31, 2020, the Division documented 3,883 FIS investigations and 1,585 IAS service requests in its case management system.

AUDIT OBJECTIVE

To assess the effectiveness* of the Division's efforts to ensure the completeness and accuracy of its case management system.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- Allegations were appropriately assigned a case number within the case management system.
- Data within selected fields was substantially complete and accurate.
- The Division manually generated reports to monitor opened and closed cases to help ensure that investigations were completed.
- Case management system access was appropriately limited by additional network based controls.
- Reportable condition related to case management system security (Finding #2).

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

FINDING #2

Improved security needed over the case management system.

The Division should improve security over its case management system to ensure that investigation information is protected from unauthorized access, modification, and disclosure.

Within the system, the Division documented 3,883 investigations of potential fraud and 1,585 IAS service requests from October 1, 2017 through May 31, 2020. Information gathered included sensitive investigation details and personally identifiable information of individuals involved.

The Division could improve security over its case management system by:

a. Requiring unique identification and authorization of system users.

   State of Michigan (SOM) Technical Standard 1340.00.080.01 requires that the agency information system owner ensures that the system uniquely identifies and authenticates system users.

b. Implementing system access authorizations to allow for the segregation of duties* or granting access based on the principle of least privilege*.

   SOM Technical Standard 1340.00.020.01 requires that the agency information system owner ensures that several baseline controls are established for an information system. These controls include, but are not limited to, the separation of duties of individuals through assigned information system access authorizations and least privilege authorizations which permit users to access only the information necessary to accomplish assigned tasks in accordance with the roles and responsibilities of their job functions.

c. Maintaining an audit log of system events.

   SOM Technical Standard 1340.00.040.01 requires that the agency information system owner ensures that the system is capable of auditing various system events.

d. Readily and safely disposing of closed investigative case files. At the time of our review, the Division identified 80,843 records within the system that were closed prior to December 31, 2009. The Division informed us that it was in the process of working with the Department of Technology, Management, and Budget to have these records purged.

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

The Department's Internal Security Records Retention and Disposal Schedule requires the disposal of closed investigation files 10 years after they are no longer active.

The Division informed us that the case management system is limited in its functionality and does not currently support these features.

RECOMMENDATION

We recommend that the Division improve security over its case management system.

AGENCY PRELIMINARY RESPONSE

The Department provided us with the following response:

The Department agrees with the recommendation and will continue its efforts to define requirements, seek funding, and establish a project to procure or develop a new case management system that complies with security requirements defined in the State of Michigan Technical Standards.

BRANCH OFFICE SAFETY AND SECURITY

BACKGROUND

The Division's Security Unit provides oversight of physical security at branch offices, including the Department's video surveillance systems, security guard contracts, and physical security alarms. The Security Unit provides operational, technical, and system support to branch office staff and FIS investigators who utilize the video surveillance system.

AUDIT OBJECTIVE

To assess the sufficiency of the Division's efforts to help ensure safety and security at branch offices.

CONCLUSION

Sufficient, with exceptions.

FACTORS IMPACTING CONCLUSION

- Department executive management, with the assistance of the Division, established a Physical Security Work Group tasked with developing security standards and establishing guidelines and best practices for physical security programs that impact branch offices.
- Every branch office has one or more types of physical security (camera systems, alarm systems, and/or security guards).
- The contractor appropriately completed monthly testing on all physical alarm systems in place at branch offices to ensure the functionality of the systems.
- The Security Unit reviewed the physical security alarm system daily activity reports and addressed all relevant concerns.
- Users with surveillance system footage access could not edit or delete footage.
- Reportable conditions related to monitoring branch office security alarm system access (Finding #3) and improving documentation of surveillance equipment maintenance (Finding #4).

FINDING #3

Improved monitoring needed over access to branch office security alarm systems.

The Division should improve its process to authorize and monitor the access codes for the security alarm systems that help to ensure safety and security at branch offices.

Sound internal control* prescribes that a supervisor should authorize a user's physical access based on the user's role and revoke access upon employee departure.

The Division assigned 398 access codes from October 1, 2017 through May 31, 2020. As of July 22, 2020, there were 49 nonemployee and 589 employee active accounts. We noted that the Division did not:

a. Document approval for 6 (30%) of 20 sampled alarm system transactions activated between October 1, 2017 through May 31, 2020.

   The Division informed us that approvals were obtained through e-mails and that this documentation was not always maintained. Also, the Division policy did not specifically address the need to document these approvals. During our audit period, the Division updated its policy to require supervisors of newly hired, transferred, or promoted branch office employees to submit a request for alarm access code form. The Division informed us that it implemented the use of this form beginning May 21, 2020.

b. Deactivate access codes in a timely manner for 37 (6%) former or inactive employees and 7 (14%) temporary contractor and administrative accounts as of July 22, 2020. One account had not been deactivated for a former employee who left the Department over 10 years ago. Our review disclosed:

Length of Time From Employee Departure to October 7, 2020 Deactivation	Number of Employees	Number of Contractor or Administrative Accounts
0 to 6 months	5	0
6 months to 1 year	13	0
Greater than 1 to 3 years	17	0
Greater than 3 years	1	0
Undeterminable	1	7
Total	37	7

The Division was not able to determine whether these individuals accessed branch offices after departure. Subsequent to our review, the Division informed us that it removed the access for these accounts.

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

The Division did not have a formal process in place to ensure that it received timely notification of employee departures. Also, although the Division policy requires it to annually audit alarm accounts for necessary updates, the policy does not provide details regarding what constitutes a necessary update. In addition, the Division informed us that limited resources impacted its ability to conduct the annual audit of active alarm accounts.

RECOMMENDATION

We recommend that the Division improve its process to authorize and monitor the access codes for the security alarm systems at branch offices.

AGENCY PRELIMINARY RESPONSE

The Department provided us with the following response:

The Department agrees with the recommendation and will continue its efforts to improve its process to authorize and monitor access codes for the security alarm systems at Secretary of State branch offices. The Department is researching alternative monitoring/reporting systems to better track the authorization and monitoring of alarm codes. The Department has added an additional position within the Enforcement Division to focus on physical security equipment issues associated with branch operations. This additional position will assist the Department in the authorization process, including the deactivation of employees, for alarm codes as well as monitoring alarm code access. The Division updated its policy to define annual audit requirements more clearly for reviewing alarm accounts.

FINDING #4

Improved documentation needed over surveillance equipment maintenance.

The Division should improve its documentation of surveillance equipment maintenance efforts to help ensure that equipment issues are resolved in a timely manner and to limit surveillance interruptions.

The Division's surveillance systems promote customer and employee safety, deter criminal behavior, and provide video footage for criminal investigations and employee disciplinary actions.

The Division uses the surveillance equipment maintenance log to track and monitor all equipment issues, such as connectivity problems and non-working equipment. Our review of this log, which included 628 equipment issues as of May 31, 2020, noted:

- 359 (57%) equipment issues did not have a documented resolution date. The Division was not able to determine when or if these issues had been resolved. Our review disclosed:

Number of Days From Notification Date	Count of Cases	Percentage of Cases
0 to 90	4	1%
91 to 180	18	5%
181 to 365	111	31%
Greater than 365	224	62%
Undeterminable	2	1%
Total	359	

- Of the 269 (43%) equipment issues with a documented resolution date, 87 (32%) were outstanding for over 180 days.

The Division indicated that the lack of a surveillance system maintenance contract and limited staff resources, both because of budget constraints, hindered its efforts to address surveillance equipment issues in a timely manner.

We noted a similar condition in our July 2017 performance audit of Bureau of Branch Office Services, Department of State (231-0333-16). In response to that audit report, the Department indicated that it agreed with the recommendation and was undertaking efforts to improve the documentation of surveillance equipment. However, our review indicated that 57% of maintenance issues recorded did not have a documented resolution date.

RECOMMENDATION

We again recommend that the Division improve its documentation of surveillance equipment maintenance efforts.

AGENCY PRELIMINARY RESPONSE

The Department provided us with the following response:

The Department agrees with the recommendation and will continue its efforts to improve documentation of surveillance equipment maintenance efforts. The Department is researching alternative monitoring/reporting systems to better track and report maintenance and repair issues. The Department has added an additional position within the Enforcement Division to focus on physical security equipment issues associated with branch operations. This additional position will assist the Department in evaluating the need for a maintenance contract or to determine that the maintenance and repairs can be timely completed and documented with existing resources.

AGENCY DESCRIPTION

The Division's mission* is to detect, reduce, and deter fraud in Department programs, as well as assist in providing a safe and secure work environment for Department personnel and facilities. This mission is carried out through a network of branch examinations, investigations, data analysis, and investigative and security support functions.

The Division is composed of the following three sections and two units:

- Branch Review and Special Programs Section (BRSPS)
  BRSPS acts as the internal review section of the Department. It conducts examinations of Secretary of State branch offices to independently assess respective responsibilities and adherence to procedures. It also conducts special examinations of allegations involving personnel suspected of fraud or procedural violations.

- Fraud Investigations Section (FIS)
  FIS investigates allegations of fraud within Department program areas, which primarily involve matters related to driver's license and vehicle fraud, including identity theft, false certification of Department documents, and title related fraud. FIS also responds to critical incidents involving safety and security events in branch offices and collaborates with law enforcement agencies in the pursuit of criminal charges when appropriate.

- Investigative Analytics Section (IAS)
  IAS provides investigation background information and conducts data analysis to assist internal Department investigators, law enforcement, and other government agency investigators.

- Insurance Fraud Prevention Unit (IFPU)
  IFPU conducts verification activities to determine whether valid vehicle insurance is presented at the time of vehicle registration. It may pursue registration and license plate cancellations due to invalid insurance and/or fraudulent insurance activity. IFPU also reports and makes recommendations on cases involving fraudulent activity to other areas within the Department as well as other areas within the State.

- Security Unit
  The Security Unit provides operational and contractual oversight of several safety and security programs pertinent to the day-to-day operations of the

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

Department, including video surveillance systems, security guard contracts, and physical security alarms.

In fiscal year 2019, the Division expended $3.0 million. As of May 31, 2020, the Division had 32 full-time employees.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

To examine records related to selected operational activities within the Division. 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 that 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, 2017 through May 31, 2020.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of the Division's operations and activities to formulate a basis for establishing our audit objectives and defining our audit scope and methodology. During our preliminary survey, we:

- Interviewed Division management and personnel regarding their functions and responsibilities.
- Reviewed applicable State laws, rules, regulations, and procedures.
- Analyzed the Division's expenditures incurred from October 1, 2017 through May 31, 2020.
- Reviewed the Division's security guard and alarm system contracts.
- Obtained an understanding of CARS.
- Reviewed a sample of IAS requests and FIS investigations to determine if the Division documented, approved, and completed requests and investigations in a timely manner.
- Completed a cursory examination of selected standard and special branch office reviews.

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

- Conducted a limited review of the Foreign Language Interpreter Program.

OBJECTIVE #1

To assess the sufficiency of the Division's efforts to deter, detect, and investigate potential fraud.

To accomplish this objective, we:

- Randomly sampled 47 of 2,584 fraud allegations received through the Division's fraud e-mail account from October 1, 2017 through May 31, 2020 to determine if selected items were accurately and timely entered into the case management system and assigned to a FIS agent or forwarded to another entity for review.

- Randomly sampled 10 of 97 standard branch office reviews, 8 of 46 special branch office reviews, and 31 of 3,883 investigations completed from October 1, 2017 through May 31, 2020 to determine if the Division appropriately documented, approved, and completed the selected items in a timely manner.

- Utilized FIS data to summarize the number of fraud allegations received from October 1, 2017 through May 31, 2020 by branch office and compared this with the standard branch reviews conducted during the same period to ensure that branch offices with 20 or more fraud allegations had been reviewed or were scheduled for review.

- Summarized CARS data for approximately 1.4 million vehicle registration transactions requiring valid insurance that occurred at branch offices from February 18, 2019 through May 31, 2020 and identified approximately 523,400 transactions referred to the IFPU, which we analyzed to determine the timeliness of the IFPU reviews.

- Randomly sampled 7 of 33 Division employees with active CARS user access as of August 19, 2020 to ensure that the access was appropriate based on the employee's assigned job functions.

We selected random samples to eliminate bias and to enable us to project the results to the respective populations.

OBJECTIVE #2

To assess the effectiveness of the Division's efforts to ensure the completeness and accuracy of its case management system.

To accomplish this objective, we:

- Interviewed Division management and personnel to discuss functionality and limitations of the case management system.
- Reviewed Division policies and SOM Technical Standards.
- Summarized and analyzed judgmentally selected fields for the 1,585 IAS and 6,509 FIS records closed from October 1, 2017 through May 31, 2020 to assess the completeness and accuracy of the case management system.

OBJECTIVE #3

To assess the sufficiency of the Division's efforts to help ensure safety and security at branch offices.

To accomplish this objective, we:

- Conducted a walkthrough of the process used to view surveillance system footage to ensure that users were not able to edit or delete footage.
- Obtained and analyzed the Division's surveillance system equipment maintenance tracking log to determine if maintenance issues were addressed timely.
- Identified the safety measures in place at each branch office and cross-referenced with the critical incidents that occurred at each branch office from October 1, 2017 through May 31, 2020 to determine if more critical incidents occurred at branches without certain safety measures.
- Randomly sampled 20 of 398 users granted alarm access codes from October 1, 2017 to May 31, 2020 to ensure that access was appropriately approved.
- Obtained a list of the 638 active alarm code accounts, as of July 22, 2020, directly from the alarm code system and compared the accounts with the Division's internal alarm access code tracking spreadsheet and payroll records to identify accounts that should be removed.
- Randomly sampled 32 of 973 daily activity reports for the physical security alarm systems from October 1, 2017 through May 31, 2020 to ensure that the Security Unit reviewed activity report events that required further attention.
- Randomly sampled 7 of 32 monthly activity reports for the physical security alarm systems from October 1, 2017 through May 31, 2020 to ensure that monthly

testing was conducted on all physical security alarm systems.

We selected random samples to eliminate bias and to enable us to 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.

AGENCY RESPONSES

Our audit report contains 4 findings and 4 corresponding recommendations. The Department's preliminary response indicates that it agrees with all of the recommendations.

The agency preliminary response that follows each recommendation in our report was taken from the Division'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.

PRIOR AUDIT FOLLOW-UP

Following is the status of the reported findings from our July 2017 performance audit of the Bureau of Branch Office Services, Department of State (231-0333-16):

Prior Audit Finding Number	Topic Area	Current Status	Current Finding Number
1	Improved documentation and monitoring of new employee training needed.	Not in scope of this audit.	
2	Improved documentation of surveillance equipment maintenance efforts needed.	Repeated*	4

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

GLOSSARY OF ABBREVIATIONS AND TERMS

BRSPS	Branch Review and Special Programs Section.
Customer and Automotive Records System (CARS)	A computer system providing services online and at Secretary of State offices, including services for vehicle owners, automotive-related businesses, driver's licenses, and ID card services.
effectiveness	Success in achieving mission and goals.
EIV	Electronic Insurance Verification.
FIS	Fraud Investigations Section.
IAS	Investigative Analytics Section.
IFPU	Insurance Fraud Prevention Unit.
internal control	The plan, policies, methods, and procedures adopted by management to meet its mission, goals, and objectives. Internal control includes the processes for planning, organizing, directing, and controlling program operations. It also includes the systems for measuring, reporting, and monitoring program performance. Internal control serves as a defense in safeguarding assets and in preventing and detecting errors; fraud; violations of laws, regulations, and provisions of contracts and grant agreements; or abuse.
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.
mission	The main purpose of a program or an entity or the reason that the program or the entity was established.
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.
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.
repeated	The same problem was noted in the current audit, and the wording of the current recommendation remains essentially the same as the prior audit recommendation.
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.
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; also known as separation of duties.
SOM	State of Michigan.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8070