# Office of the Auditor General
Performance Audit Report

# MDOT Grant System
Michigan Department of Transportation and
Department of Technology, Management, and Budget

December 2017

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

591-0593-17

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*

## *MDOT Grant System (MGS)*

## *Michigan Department of Transportation (MDOT) and Department of Technology, Management, and Budget (DTMB)*

**Report Number:**
**591-0593-17**

**Released:**
**December 2017**

MGS is used by MDOT's Office of Economic Development (OED) to collect, track, rank, analyze, and preliminarily approve grants to county road commissions, cities, villages, State agencies, transit agencies, and Native American tribes. OED administers grants to enhance the State's intermodal transportation system and ability to compete in a global economy. MGS is a Web-based system that allows grant applicants to electronically submit applications, track grant application progress, communicate with MDOT grant administrators, and upload supporting documentation. From October 1, 2016 through June 30, 2017, OED received 132 grant applications and awarded 91 grants totaling $50.0 million.

| Audit Objective | | | Conclusion |
|---|---|---|---|
| Objective #1: To assess the effectiveness of MDOT and DTMB's security and access controls over MGS. | | | Moderately effective |
| **Findings Related to This Audit Objective** | **Material Condition** | **Reportable Condition** | **Agency Preliminary Response** |
| MGS needs more fully established and implemented access controls. Of the 65 users with edit capabilities, 18 (28%) had access rights in excess of those necessary to perform their jobs and 8 were departed users (Finding #1). | | X | Agrees |
| MGS information needs to be better protected against unauthorized use, disclosure, modification, or destruction with improved security controls. MDOT did not conduct and document an MGS risk assessment, security assessment plan, or contingency plan (Finding #2). | | X | Agrees |
| MGS did not contain controls to help prevent and detect inappropriate grant application approvals, which increased the risk that someone other than the OED administrator could preliminarily approve a grant application without being detected (Finding #3). | | X | Agrees |

| Audit Objective | | | Conclusion |
|---|---|---|---|
| Objective #2: To assess the effectiveness of MDOT's efforts to ensure the accuracy and completeness of MGS data. | | | Effective |
| **Findings Related to This Audit Objective** | **Material Condition** | **Reportable Condition** | **Agency Preliminary Response** |
| None reported. | Not applicable. | | |

**Obtain Audit Reports**

Online: audgen.michigan.gov

Phone: (517) 334-8050

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

**Doug A. Ringler, CPA, CIA**
Auditor General

**Laura J. Hirst, CPA**
Deputy Auditor General

OAG
Office of the Auditor General

**Doug A. Ringler, CPA, CIA**
Auditor General

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

December 12, 2017

Mr. Todd Wyett, Chair
State Transportation Commission
and
Kirk T. Steudle, PE, Director
Michigan Department of Transportation
Murray D. Van Wagoner Building
Lansing, Michigan
and
Mr. David L. DeVries
Director, Department of Technology, Management, and Budget
Chief Information Officer, State of Michigan
Lewis Cass Building
Lansing, Michigan

Dear Mr. Wyett, Mr. Steudle, and Mr. DeVries:

This is our performance audit report on the MDOT Grant System, Michigan Department of Transportation (MDOT) and Department of Technology, Management, and Budget.

We organize our findings and observations by audit objective. MDOT 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

## MDOT GRANT SYSTEM

This Page Left Intentionally Blank

# AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

## SECURITY AND ACCESS CONTROLS OVER MGS

**BACKGROUND**

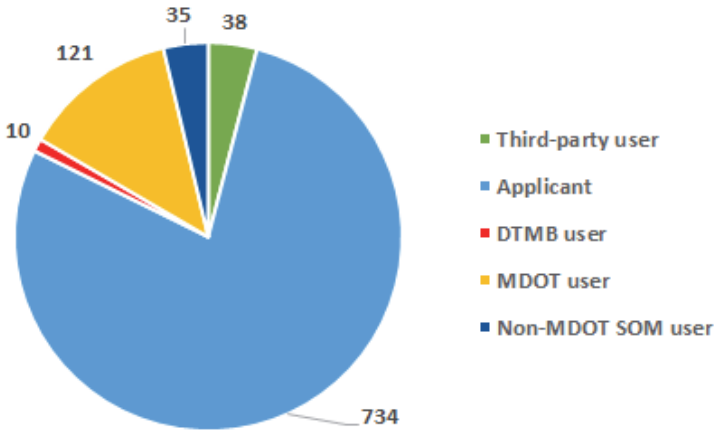
The MDOT Grant System (MGS) security* and access controls* limit and detect inappropriate access, which is important to ensure the availability, confidentiality, and integrity* of data.

The State of Michigan (SOM) has adopted the security controls identified in the National Institute of Standards and Technology* (NIST) Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, as the set of controls for SOM information systems. The Department of Technology, Management, and Budget (DTMB) developed technical standards for each NIST security control group, which are modified in some cases for SOM implementation. DTMB technical standards are applicable to all SOM networks, systems, computers, data, databases, and applications and supersede all security standards that may be in conflict with them.

The Federal Information System Controls Audit Manual* (FISCAM) is a methodology developed by the U.S. Government Accountability Office (GAO) for performing information system control audits of governmental entities in accordance with professional standards.

MGS is used by the Office of Economic Development (OED), Michigan Department of Transportation (MDOT), to collect, track, rank, analyze, and preliminarily approve grants to county road commissions, cities, villages, State agencies, transit agencies, and Native American tribes. OED administered grants enhance the State's intermodal transportation system and ability to compete in a global economy.

As of August 7, 2017, there were 938 MGS users as follows:




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

| | |
|---|---|
| **AUDIT OBJECTIVE** | To assess the effectiveness* of MDOT and DTMB's security and access controls over MGS. |
| **CONCLUSION** | Moderately effective. |
| **FACTORS IMPACTING CONCLUSION** | • No identified instances of inappropriate user access to MGS data.<br>• MGS does not contain confidential or sensitive information.<br>• Reportable conditions* related to improved MGS user access controls, more comprehensive security controls, and improved grant application approval controls (Findings #1 through #3). |

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

## FINDING #1

**Improved MGS user access controls are needed.**

MDOT, in conjunction with DTMB, did not fully establish and implement user access controls over MGS to ensure the authorization and authentication of users and the protection of MGS data.

FISCAM states that user access should be limited to individuals with a valid business purpose, access authorization forms should be maintained, access rights should prevent conflicting transactions and activities, and system owners and security managers should periodically monitor user access.

MDOT, in conjunction with DTMB, did not:

a. Employ the principle of least privilege*.

   Of the 65 MGS users with edit capabilities, 18 (28%) were granted access rights in excess of those necessary to perform their assigned job functions. Examples include:

   - Seven users had administrative rights to oversee and process applications for grants that they did not manage.

   - Six users had administrative rights to assign tasks to grant coordinators, technical reviewers, and applicants. This capability should be limited to OED program support staff and management.

   Failure to employ least privileged access could weaken the integrity of MGS data and the grant application review process if inappropriate individuals edit data outside the purview of their assigned job function.

b. Remove MGS access of departed users in a timely manner.

   DTMB requires system access removal within 24 hours of user termination or transfer. Of the 8 departed users with edit capabilities, MDOT did not promptly deactivate any of their user accounts. Four of the 8 departed users were MDOT employees that MDOT took between 16 and 116 days to deactivate. Without prompt deactivation, unauthorized individuals could access and edit MGS data.

c. Use standard authorization forms to document OED approval of the access rights granted to users.

   The information system owner* and two MGS system administrators assign user access; however, they did not document the business purpose for granting those access rights. Documenting this authorization helps ensure that

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

only appropriate individuals obtain access to MGS and that the rights assigned are appropriate.

d. Periodically review user access rights every 120 days.

   MDOT had not reviewed user access rights since MGS was implemented in October 2012. Without periodic review, MDOT is unable to determine if initial access rights granted to users continue to remain appropriate.

e. Automatically disable inactive user accounts after 60 days.

   As of August 7, 2017, MDOT had not disabled user accounts for any of the 722 inactive users. MGS has the capability to track and monitor a user's last access date; however, that function was not activated until May 2017. Failure to automatically disable inactive user accounts exposes MGS to the risk of unauthorized access.

**RECOMMENDATION**

We recommend that MDOT, in conjunction with DTMB, fully establish and implement user access controls over MGS to help ensure the authorization and authentication of users.

**AGENCY PRELIMINARY RESPONSE**

MDOT provided us with the following response:

*MDOT agrees with parts a. through d., and, although MDOT identified no suspicious MGS activity or compromised data, it will continue to establish and implement improved and cost-effective user access controls over MGS.*

*While MDOT agrees that it did not follow the requirements discussed in part e. of the finding, it is not cost-effective to automatically disable user accounts labeled "inactive" by the 60-day standard. There are hundreds of annual applicants that might apply for applicable grants. MGS was specifically designed to allow periodic access that exceeds the 60-day standard by those applicants. Also, MGS user roles were created and appropriately limited to mitigate the same risk the standard was designed to mitigate. In addition, MDOT manages user access in System Access Manager.*

## FINDING #2

**More comprehensive security controls are needed.**

MDOT, in conjunction with DTMB, did not fully implement security controls to protect MGS information from unauthorized use, disclosure, modification, or destruction and to ensure the integrity and availability of MGS information.

DTMB Administrative Guide policy 1340.00 requires State agencies to implement Michigan Cyber Security (MCS) baseline controls. The MGS information technology project security plan and assessment (DTMB-0170*) also identifies appropriate security controls that MDOT and DTMB should implement.

MDOT, in conjunction with DTMB, did not:

a. Conduct, retain, and review a risk assessment of MGS and the information that it processes, stores, and transmits as required by DTMB Technical Standard 1340.00.150.01.

   The MCS security liaison should have completed a risk assessment during MGS implementation and documented it as a component of the DTMB-0170 process. In addition, MDOT should have reviewed the risk assessment results at least annually. MDOT indicated that the DTMB project manager likely completed an MGS risk assessment; however, neither MDOT nor DTMB was able to locate it. A risk assessment is important to ensure that MDOT identifies and addresses security vulnerabilities and threats that could impact MGS security.

b. Create and implement a security assessment plan or perform security tests during MGS development as required by DTMB Technical Standard 1340.00.160.01.

   A security assessment plan and associated security tests and evaluations help ensure that required MGS security controls are implemented correctly, operating as intended, enforcing the desired security plan, and meeting established security requirements.

c. Establish and test an MGS contingency plan at least annually as required by DTMB Technical Standard 1340.00.070.01.

   MDOT informed us that it did not establish a contingency plan because it did not identify MGS as a business critical application. A contingency plan is necessary to ensure the availability of critical information resources and continuity of operations in emergency situations. Also, annual testing of the contingency plan is important to determine the effectiveness and organizational readiness to execute the plan.

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

**RECOMMENDATION**

We recommend that MDOT, in conjunction with DTMB, fully implement security controls to protect MGS information from unauthorized use, disclosure, modification, or destruction.

**AGENCY PRELIMINARY RESPONSE**

MDOT provided us with the following response:

*MDOT agrees with sections a. and b. of the finding, although the finding does not identify instances of unauthorized use, disclosure, modification, or destruction of data.*

*MDOT intends to complete a new risk and security assessment using the new State of Michigan software, Lockpath.*

*Although MDOT agrees that it did not follow the requirements discussed in section c. of the finding, MDOT chose not to expend resources to establish contingency plans for all 200+ MDOT productions systems.*

## FINDING #3

**Controls over grant application approvals could be improved.**

MDOT, in conjunction with DTMB, did not fully establish controls in MGS to help prevent and detect inappropriate grant application approvals, increasing the risk that someone other than the OED administrator could preliminarily approve a grant application without being detected.

OED's grant award process requires a user with an "Administrator for the Office of Economic Development" (AOED) user role to approve each grant application in MGS prior to formally awarding a grant. DTMB Technical Standard 1340.00.020.01 requires the information system owner to specify MGS authorized users, role membership, and authorized access.

MDOT, in conjunction with DTMB, did not:

a. Design and configure MGS to document the identity of the user who approved each grant application.

   The OED administrator is the only individual authorized to approve grant applications in MGS. Without a documented approval record, OED cannot determine if someone other than the OED administrator approved grant applications.

b. Restrict the AOED user role to only the OED administrator.

   In addition to the OED administrator, the MGS information system owner was also assigned the AOED user role and had the ability to approve grant applications. Subsequent to informing OED of the inappropriate AOED user role assignment, it removed AOED access from the information system owner.

c. Ensure that only appropriate system administrators could assign the AOED user role.

   In addition to the MGS information system owner and his/her backup, one additional non-OED user had the ability to assign and remove the AOED user role to any MGS user.

**RECOMMENDATION**

We recommend that MDOT, in conjunction with DTMB, fully establish controls in MGS to help prevent and detect inappropriate grant application approvals.

**AGENCY PRELIMINARY RESPONSE**

MDOT provided us with the following response:

*MDOT agrees with the finding and, although MDOT identified no suspicious MGS activity or compromised data, it will continue its efforts to establish applicable cost-effective controls in MGS. Also, outside of MGS, as a compensating operational control, MDOT's Director approves all applicable grants.*

## ACCURACY AND COMPLETENESS OF MGS DATA

**BACKGROUND**

MDOT ensures the accuracy and completeness of MGS data through automated system edits and independent manual checks of grant information by program staff during the grant project closure process.

Grant applicants include county road commissions, cities, villages, State agencies, transit agencies, and Native American tribes. Applicants prepare and submit applications electronically in MGS. OED program managers and grant coordinators work with applicants and technical reviewers throughout the application process to ensure the accuracy and completeness of applications. MDOT generally selects grant award recipients based on the recommendations of an application review committee and scores calculated in MGS. Final approvals of grant awards are completed by the OED Director (within MGS) and the MDOT Director.

OED enters grant project information into MDOT's accounting system, Michigan Financial Obligation System (MFOS), after the grant application review and approval process is completed in MGS. MDOT project managers monitor and document project progress in MFOS until the completion of all project job phases. After the grant project is complete, final project costs from MFOS are interfaced with MGS and OED closes the grant in MGS.

**AUDIT OBJECTIVE**

To assess the effectiveness of MDOT's efforts to ensure the accuracy and completeness of MGS data.

**CONCLUSION**

Effective.

**FACTORS IMPACTING CONCLUSION**

- No significant data integrity weaknesses identified related to the grant application process.
- No significant weaknesses identified in the Transportation Economic Development Fund (TEDF) category A or category F scoring report process.

# SUPPLEMENTAL INFORMATION

UNAUDITED

MDOT GRANT SYSTEM
Office of Economic Development Grants Awarded
October 1, 2014 Through June 30, 2017

| | Fiscal Year | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 2015 | | 2016 | | 2017 (Through June 30, 2017) | | Total | |
| | Number of Grants Awarded | Total Amount | Number of Grants Awarded | Total Amount | Number of Grants Awarded | Total Amount | Number of Grants Awarded | Total Amount |
| TEDF - Category A | 38 | $14,854,948 | 37 | $19,003,742 | 17 | $ 9,180,815 | 92 | $ 43,039,505 |
| TEDF - Category F | 8 | 2,405,714 | 9 | 2,511,683 | 10 | 2,805,423 | 27 | 7,722,820 |
| TAP* | 68 | 31,559,687 | 62 | 36,118,861 | 63 | 37,586,860 | 193 | 105,265,409 |
| SRTS Program* | 3 | 1,100,740 | 0 | 0 | 1 | 387,031 | 4 | 1,487,771 |
| Total | 117 | $49,921,089 | 108 | $57,634,286 | 91 | $49,960,129 | 316 | $157,515,505 |

*SRTS became a component of the TAP program effective October 1, 2012. Grants awarded by the SRTS Program in fiscal years 2015 and 2017 are due to unexpended pre-October 1, 2012 program funds becoming available.

Source: MDOT Office of Economic Development.

## SYSTEM DESCRIPTION

MGS is a Web-based system used by MDOT's OED to collect, track, rank, analyze, and preliminarily approve State and federally funded grant applications for the following grants administered by OED:

- TEDF category A and F grants
- Transportation Alternatives Program (TAP) grants
- Safe Routes to School (SRTS) grants

TAP and SRTS are federally funded programs. All OED grants are competitive except for TEDF category F grants. In fiscal year 2017 (through June 30, 2017), OED received 132 grant applications and awarded 91 grants totaling $50.0 million (see supplemental information).

MGS was implemented in October 2012 for TAP and SRTS grants and in April 2014 for TEDF grants. MGS eliminated the need for hard-copy documentation because applicants create and submit applications online. MGS was developed by DTMB as an add-on application for MDOT's accounting system, MFOS. MGS interfaces with MDOT's JobNet system and MFOS to validate the accuracy and completeness of grant applications.

## AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

**AUDIT SCOPE**

To examine the information processing and other records of MGS. 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 October 1, 2014 through June 30, 2017.

**METHODOLOGY**

We conducted a preliminary survey of MGS to formulate a basis for defining our audit objectives and scope. During our preliminary survey, we:

- Interviewed MDOT management and staff to obtain an understanding and a walk-through of MGS.
- Reviewed MDOT and DTMB policies and procedures related to MGS and MGS security.
- Reviewed system documentation, including the MGS security plan and assessment, network diagram, data dictionary, and user guide.
- Reviewed FISCAM and NIST Special Publication 800-53 to obtain an understanding of information system control standards.
- Obtained an understanding of MDOT's processes for:
    - Granting access to MGS.
    - Determining the roles and privileges assigned to users.
    - Ensuring the accuracy and completeness of MGS data output.

**OBJECTIVE #1**

To assess the effectiveness of MDOT and DTMB's security and access controls over MGS.

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

To accomplish this objective, we:

- Obtained a list of active MGS users and assessed whether MDOT:
  - Followed the principle of least privilege when assigning roles and privileges to users.
  - Timely deactivated user accounts of terminated employees and third-party users.
  - Timely deactivated user accounts of employees who no longer had a valid business purpose to access MGS.
  - Implemented access authorization policies and procedures.
  - Periodically reviewed user access rights.
  - Automatically disabled inactive user accounts.
- Reviewed system documentation to determine if MDOT and DTMB completed and documented an MGS risk assessment, security plan, and contingency plan.
- Validated that grant approval business rules were properly enforced within MGS.
- Reviewed data input to ensure that confidential information was not entered into MGS.

**OBJECTIVE #2**

To assess the effectiveness of MDOT's efforts to ensure the accuracy and completeness of MGS data.

To accomplish this objective, we:

- Replicated selected TEDF category A and category F scoring reports to ensure that MGS accurately calculated grant application scores.
- Validated that grant-related project costs in MFOS accurately interfaced into MGS.
- Reviewed the accuracy of data entered into MGS.
- Validated the completeness and accuracy of pre-programmed and ad hoc MGS reports.

**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 3 findings and 3 corresponding recommendations. MDOT's preliminary response indicated that it agrees with all 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 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 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.

**SUPPLEMENTAL INFORMATION**

Our audit report includes supplemental information. Our audit was not directed toward expressing a conclusion on this information.

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

## 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. |
| **AOED** | Administrator for the Office of Economic Development. |
| **DTMB** | Department of Technology, Management, and Budget. |
| **DTMB-0170** | A document establishing an information system security plan and risk assessment for evaluating the security controls in place or planned for a system. |
| **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 system owner** | Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. |
| **integrity** | Accuracy, completeness, and timeliness of data in an information system. |
| **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. |
| **MCS** | Michigan Cyber Security. |
| **MDOT** | Michigan Department of Transportation. |
| **MFOS** | Michigan Financial Obligation System. |
| **MGS** | MDOT Grant System. |

| | |
|---|---|
| **National Institute of Standards and Technology (NIST)** | An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs. |
| **OED** | Office of Economic Development. |
| **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. |
| **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. |
| **SOM** | State of Michigan. |
| **SRTS** | Safe Routes to School. |
| **TAP** | Transportation Alternatives Program. |
| **TEDF** | Transportation Economic Development Fund. |

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) 334-8060, Ext. 1650