Office of the Auditor General
Performance Audit Report

MiConnect: Hunting, Fishing, and Recreational Licensing System

Department of Natural Resources

September 2026

751-0590-25

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

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
MiConnect: Hunting, Fishing, and Recreational Licensing System
Department of Natural Resources (DNR)

Report Number:
751-0590-25

Released:
September 2026

DNR established and maintains the MiConnect system which is used for the sale and purchase of hunting, fishing, snowmobile, and off-road vehicle licenses. Also, MiConnect is used for hunting lottery applications, fuelwood permits, Outdoor Skills Academy classes (e.g., fishing clinics, hunting clinics, and survival classes), and deer harvest patches. For fiscal year 2024, 2.3 million transactions were processed totaling $79.7 million; for fiscal year 2025, 2.4 million transactions were processed totaling $86.4 million. As of July 30, 2025, MiConnect had 3,947 active user accounts consisting of DNR employees, vendor employees, and retailers.

Audit Objective			Conclusion
Objective 1: To assess the effectiveness of DNR's security and user access controls over the MiConnect application and data.			Moderately effective
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
DNR did not document its approval for any of the 22 new MiConnect user accounts during our audit period. Also, DNR did not automatically disable 43 (11%) of 376 inactive internal accounts and 565 (16%) of 3,545 inactive external point-of-sale accounts after 60 days of inactivity, ranging from 61 to 1,988 days (Finding 1).	X		Agrees

Audit Objective			Conclusion
Objective 2: To assess the sufficiency of DNR's monitoring efforts of MiConnect's third-party service organization (TPSO).			Sufficient, with exceptions
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
DNR did not review and test 100% of its user entity responsibilities related to its control environment and operational effectiveness, which can undermine the intended benefits of third-party service organizations (Finding 2).		X	Agrees

Audit Objective			Conclusion
Objective 3: To assess the sufficiency of DNR's efforts to ensure the completeness and accuracy of data within MiConnect.			Sufficient, with exceptions
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
To prevent customers from purchasing multiple licenses, DNR needs an effective process to ensure duplicative customer accounts are removed (Finding 3).		X	Agrees

Audit Objective			Conclusion
Objective 4: To assess the sufficiency of DNR's efforts to implement change controls over the MiConnect application and data.			Sufficient, with exceptions
Findings Related to This Audit Objective	**Material Condition**	**Reportable Condition**	**Agency Preliminary Response**
Change control documentation was not maintained for 100% of user acceptance testing and post-implementation validation changes (Finding 4).		X	Agrees

Audit Objective			Conclusion
Objective 5: To assess the effectiveness of DNR's interface controls over MiConnect.			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

September 1, 2026

Rebecca A. Humphries, Chair
Natural Resources Commission
and
M. Scott Bowen, Director
Department of Natural Resources
Deborah A. Stabenow Building
Lansing, Michigan

Chair Humphries and Director Bowen:

This is our performance audit report on MiConnect: Hunting, Fishing, and Recreational Licensing System, Department of Natural Resources.

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* require an audited agency to develop a plan to comply with the recommendations and submit it to the State Budget Office (SBO) upon audit completion. State administrative procedures require the audited agency to develop the plan as early as practicable and within 60 days after report issuance and submit the plan to the Office of Internal Audit Services (OIAS), SBO. Within 30 days of receipt, OIAS will 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

MICONNECT: HUNTING, FISHING, AND RECREATIONAL LICENSING SYSTEM

This Page Left Intentionally Blank

AUDIT OBJECTIVES, CONCLUSIONS, FINDINGS, AND OBSERVATIONS

SECURITY AND ACCESS CONTROLS OVER THE MICONNECT APPLICATION AND DATA

BACKGROUND

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

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

The primary users of MiConnect consist of Department of Natural Resources (DNR) employees and point-of-sale (POS) users employed by licensed agents who access the system via a terminal provided by DNR. As of July 30, 2025, MiConnect had 3,947 active users.

According to the State of Michigan Financial Management Guide* (FMG) (Part VII, Chapter 1, Section 900), DNR has the primary responsibility for establishing, maintaining, and monitoring internal control* over its critical IT applications.

AUDIT OBJECTIVE

To assess the effectiveness* of DNR's security and user access controls over the MiConnect application and data.

CONCLUSION

Moderately effective.

FACTORS IMPACTING CONCLUSION

- Some access controls and security configuration parameters were implemented in accordance with State policies and standards.
- DNR established and implemented some procedures related to user account authorization in accordance with State policies and standards.
- MiConnect users reviewed did not have incompatible roles.
- One material condition* related to fully implementing effective user security and access controls (Finding 1).

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

FINDING 1

Improvements to user access needed.

DNR did not fully establish and implement a number of security and access controls over MiConnect, which could result in unauthorized access, disclosure, modification, or destruction of customer data.

State of Michigan (SOM) Technical Standard 1340.00.020.01 defines the security control baselines for access to information systems. It requires State agencies to implement, monitor, and document processes approved by the Department of Technology, Management, and Budget (DTMB) and be compliant with the National Institute of Standards and Technology* (NIST) guidance to create, enable, modify, disable, and remove system accounts.

Our review of the MiConnect system noted DNR did not:

a. Automatically disable user accounts after 60 days of inactivity. We reviewed 376 active internal and 3,545 active external POS accounts as of July 30, 2025 and determined DNR did not disable:

   (1) 43 (11%) inactive internal accounts and 565 (16%) inactive external POS accounts with MiConnect access. On average, these users did not log into MiConnect for 230 days, with last log-in times ranging from 61 to 1,988 days.

   (2) Access for user accounts which never logged in after account creation for 9 (2%) internal and 609 (17%) external POS MiConnect user accounts. On average, these accounts were created 1,318 days prior to July 30, 2025, with creation times ranging from 64 to 2,016 days.

   SOM Technical Standard 1340.00.020.01 requires an information system to automatically disable user accounts after 60 days of inactivity.

b. Implement an effective process to timely remove access for users who separated from DNR employment. Other DNR divisions did not notify the system administrator in a timely manner for 11 (92%) of 12 sampled users who separated from employment. Therefore, the users were deactivated an average of 178 days late. Also, 1 (9%) of the 11 users noted above was not removed within three days of notification of employment separation.

   SOM Technical Standard 1340.00.020.01 requires agencies to remove access within three business days when users end employment.

   DNR policy requires management to notify the MiConnect system administrator when a user's employment ends.

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

However, managers often delay the notification until the system administrator completes quarterly recertification.

c. Implement an effective process to evaluate and recertify user access. We sampled 34 (6%) of 532 non-privileged internal user accounts, all 5 privileged user* accounts, and the 5,366 external POS accounts active during our audit period and compared them to the quarterly recertifications completed from October 1, 2023 through July 30, 2025. Our review noted:

   (1) 27 (79%) of 34 sampled non-privileged internal users active at some point during the audit period were not annually recertified.

   (2) All 5 of the sampled privileged users active at some point during the audit period were not certified semiannually.

       DNR provided documentation to support the completion of 3 of 7 quarterly recertifications during the audit period. However, when DNR e-mailed the division managers, they provided negative confirmation and only requested a response if a user's access should be removed.

   (3) Recertifications did not include all active external POS users employed by licensed agents.

       Once an agent becomes licensed, the POS retail agent contract requires them to manage user access for their employees. However, the contract does not require the agents to complete annual recertifications, and DNR does not monitor agents to ensure they are annually recertifying users.

   SOM Technical Standard 1340.00.020.01 requires a review of accounts through a semiannual certification of privileged accounts, and annual certification of all other accounts, to verify they are still required.

d. Consistently perform effective user account management. We sampled 22 users granted access to MiConnect from October 1, 2023 through July 30, 2025 and noted DNR did not:

   (1) Document the MiConnect access requested and approved for 22 (100%) user accounts. Specifically:

       (a) 3 (14%) did not have an access authorization form.

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

DNR did not document system administrator or security administrator approvals for 86% of MiConnect users.

(b) 19 (86%) access authorization forms were incomplete and did not document the approval signature of the system administrator or the security administrator.

(2) Ensure access was granted based on the principle of least privilege*. Inappropriate access to MiConnect privileged functions was granted to 1 (5%) user.

SOM Technical Standard 1340.00.020.01 requires State agencies to establish a process to control and document the assignment of access rights based on current job responsibilities and principle of least privilege.

e. Implement an effective process to identify incompatible roles or excessive access rights within MiConnect to ensure segregation of duties* and the access granted is based on the principle of least privilege. We noted DNR did not maintain sufficient documentation to support its assessment of incompatible roles. However, while some users had multiple roles, we did not identify any users with incompatible roles.

f. Ensure security configurations were appropriate. Because of the confidentiality of these configurations, we are noting this issue in the finding and providing the underlying details to DNR management.

For parts a. through f., DNR informed us it did not have sufficient processes and controls to ensure compliance with SOM technical standards.

We consider this to be a material condition because of the considerable exception rate related to the lack of approvals for new user access, the lack of documentation for privileged and non-privileged user recertification, the number of inactive users and the duration of inactivity, and the timeliness of access removal after employment separation.

RECOMMENDATION

We recommend DNR fully establish and implement security and access controls over MiConnect.

AGENCY PRELIMINARY RESPONSE

DNR provided us with the following response:

DNR agrees with the recommendation. DNR understands and acknowledges the finding and will implement user access controls to ensure that inactive accounts are disabled in accordance with SOM Technical Standards.

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

MONITORING OF THIRD-PARTY SERVICE ORGANIZATIONS

BACKGROUND

In October 2018, DNR and DTMB engaged a third-party service organization (TPSO) for a commercial off-the-shelf* (COTS) solution, which included maintenance, support, and enhancement of MiConnect. The application is vendor hosted using a third-party cloud service provider application.

According to the FMG (Part VII, Chapter 1, Section 1000) each department is required to establish and maintain a sound internal control system over activities, including those managed by TPSOs. To ensure the State's interests are protected in an acceptable fashion, the department should consider the TPSO's significance to department operations, gain an understanding of the TPSO's controls, and obtain assurance the controls are present and functioning as intended. The FMG adds, a System and Organization Controls* (SOC) report can be obtained to provide departments with an opinion, a conclusion, or findings regarding the reliability of controls related to services.

Also, the FMG requires departments to obtain a bridge letter issued by the senior management with operating responsibility of the TPSO for any gaps between their report date and the user organization's fiscal year-end. The bridge letter makes the following assertions: the control environment described in the SOC report has not changed and the tested controls continued to operate effectively during gaps between the reporting period and the State of Michigan's fiscal year.

MiConnect houses customers' personally identifiable information* (PII) and financial information. For this information, monitoring the TPSO SOC report is essential for obtaining assurance regarding the reliability of controls in place at the TPSO.

AUDIT OBJECTIVE

To assess the sufficiency of DNR's monitoring efforts of MiConnect's TPSO.

CONCLUSION

Sufficient, with exceptions.

FACTORS IMPACTING CONCLUSION

- DNR obtained, reviewed, and submitted the TPSO's SOC report and its review within the required timelines set by the FMG for the most recent SOC report period.
- DNR obtained a bridge letter for the most recent SOC report period.

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

- One reportable condition* related to improving TPSO SOC report monitoring and implementing controls to manage risks associated with services provided by a TPSO (Finding 2).

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

FINDING 2

Improvements needed for monitoring TPSOs.

DNR should continue to improve its monitoring over the MiConnect TPSO through better understanding of its SOC report review responsibilities. Strengthened monitoring would increase DNR's assurance regarding the security, collection, and management of customer and financial information.

SOC reports are internal control reports on the services provided by a TPSO. The reports provide valuable information users need to assess and address the risks associated with a TPSO. DNR's contract requires the vendor to annually provide a SOC 2, type 2 report, which evaluates the vendor's protection of DNR data relevant to security, availability, processing integrity, confidentiality, and privacy.

The FMG (Part VII, Chapter 1, Section 1000) prescribes guidelines for departments to assess and manage risks associated with TPSOs. Also, it requires each agency to establish and maintain a sound internal control system over activities and transactions, including those managed by TPSOs. The FMG requires each department to obtain third-party assurance reports within 60 days of the report issue date.

According to the FMG, departments need to evaluate the risks and controls under which each service organization designs, implements, and operates for the assigned operational process, and how the service organization's internal control system impacts the department's internal control system. Also, it requires the department to review the SOC report, which includes using the SOC Report Review Template to evaluate and review the auditor's opinion, management's assertion of the control environment, and use of subservice organizations. In addition, departments should consider and document conclusions regarding whether a TPSO's controls are relevant to the department's control environment.

We reviewed MiConnect SOC 2, type 2 reports to evaluate DNR's monitoring efforts of the TPSO and noted instances in which DNR did not:

a. Obtain the report in a timely manner. DNR obtained the report 300 days after the issue date and thereby did not promptly submit its report review to the Office of Internal Audit Services, State Budget Office.

b. Obtain a bridge letter to address coverage gaps between the reporting period and the State's fiscal year-end.

DNR did not review and test the 12 user entity responsibilities listed in the SOC report.

c. Review and test the 12 user entity responsibilities* outlined in the corresponding SOC report.

d. Obtain and/or document a review of the TPSO's subservice organization's SOC report. Therefore, DNR

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

did not consider whether the subservice controls were relevant to the department's control environment. Our review of the report disclosed an evaluation of the design, implementation, or operational effectiveness of the subservice organization's controls was specifically excluded in the scope of the report. The vendor uses subservice organizations to provide data center hosting and infrastructure. Without reviewing the subservice organization SOC report, DNR is unable to consider whether the subservice controls were relevant to the department's control environment.

DNR informed us it misunderstood its responsibilities regarding the evaluation of the SOC reports and how to implement effective compensating controls, if needed, to ensure DNR derives full value from the services provided.

RECOMMENDATION

We recommend DNR continue to improve its monitoring of the MiConnect TPSO.

AGENCY PRELIMINARY RESPONSE

DNR provided us with the following response:

DNR agrees with the recommendation. The root cause was an internal misunderstanding of the DNR's specific responsibilities regarding the comprehensive evaluation of the SOC report's scope and contents, particularly the review of controls outlined in the User Entity Responsibilities section. DNR will make the necessary internal adjustments to our process to ensure we are appropriately monitoring our third-party service organization for MiConnect.

COMPLETENESS AND ACCURACY OF DATA

BACKGROUND

According to the Federal Information System Controls Audit Manual (FISCAM), controls should be implemented to provide reasonable assurance of the completeness and accuracy of data within a system.

From October 1, 2023 through July 25, 2025, 1.9 million unique customer IDs purchased 9.6 million products* in MiConnect. Products are often limited, restricted, or discounted per the Natural Resources and Environmental Protection Act (Public Act 451 of 1994).

DNR relies on customers and authorized agents to accurately enter required customer information to ensure customers receive the appropriate product and pricing. Required information includes first and last names, date of birth, addresses, and customer declarations (i.e., Michigan resident, legally blind, active U.S. military status, and disabled veteran status).

MiConnect interfaces with the Department of State (DOS) to update any differing customer information (e.g., date of birth, name, and address) when compared to what the customer or agent entered into MiConnect. The interface may update a customer record in MiConnect if there is a matching Michigan driver's license number.

AUDIT OBJECTIVE

To assess the sufficiency of DNR's efforts to ensure the completeness and accuracy of data within MiConnect.

CONCLUSION

Sufficient, with exceptions.

FACTORS IMPACTING CONCLUSION

- As of July 25, 2025, customer data within MiConnect materially matched DOS driver's license records for customers who purchased a DNR license during the audit period.
- As of July 25, 2025, customers received appropriate resident or nonresident restricted purchases for our sample of customers who purchased a license during the audit period.
- One reportable condition related to implementing an effective process to remove potentially duplicative customer accounts (Finding 3).

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

FINDING 3

Process needed to review duplicate customer accounts.

DNR did not fully establish and implement an effective process to remove potentially duplicative customer accounts which could result in customers circumventing license purchase limits.

Section 324.40107 of the *Michigan Compiled Laws* states the department shall manage all animals in this State and may issue orders to determine the kinds of animals which may be taken, establish lawful methods of taking game, establish bag limits, determine the conditions under which permits may be issued, and establish fees for the issuing of permits.

The FMG (Part VII, Chapter 1, Section 900) states the department, as the IT application and data owner, has primary responsibility for designing, implementing, and conducting application internal controls and assessing their effectiveness. Application controls are embedded in business processes to ensure information is complete, accurate, valid, and authorized.

DNR's automatic merge process for duplicate customer accounts does not consider accounts with spelling errors.

DNR has a process in place to automatically merge duplicate customer accounts if the first name, last name, date of birth, residence city, and residence zip code match. If any differences exist between the fields, accounts are not merged. Also, DNR has a manual merge process where various DNR staff run reports to assess the same five fields and determine if merging the customer accounts is appropriate. However, this is an informal and undocumented process. The informal process does not define critical elements such as:

- Responsible parties for performing the manual merge review.
- A standardized process for all staff to follow.
- Frequency of performing the review.
- Which reports to utilize.

As of July 25, 2025, we analyzed all 1.9 million unique customers who purchased a license during our audit period and identified:

a. 176 duplicate driver's license numbers associated with more than one customer. We sampled 18 driver's license numbers and found 6 (33%) were for the same customer who had more than one account.

   The customers' accounts had minor differences which included transposed names, spelling errors in city names (Raleigh vs. Raliegh), and spaces in out-of-country zip codes (P6C6A8 vs. P6C 6A8).

b. 4,110 duplicate name and date of birth combinations associated with more than one customer account. We sampled 33 name and date of birth combinations for

further review and found 7 (21%) were for the same customer who had more than one account.

The customers' accounts had minor differences which included spelling errors in city names (Wapuan vs. Waupun), different but similar city names (Washington vs. Washington Township), and different city names but same street addresses.

DNR informed us it does not have sufficient processes in place to ensure customers do not have multiple accounts, which could allow customers to purchase duplicate licenses.

RECOMMENDATION

We recommend DNR fully establish and implement an effective process to remove potentially duplicative customer accounts within MiConnect.

AGENCY PRELIMINARY RESPONSE

DNR provided us with the following response:

DNR agrees with the recommendation. DNR acknowledges that customer user errors are a common contributing factor to this issue. The department will develop enhanced detection and consolidation methods to address duplicate accounts within the system.

CHANGE CONTROLS

BACKGROUND

Changes to MiConnect are typically initiated when DNR authorizes a needed modification to update or modify the application. The TPSO constructs the change in a development environment, and it is then moved to a test environment in which the change undergoes quality assurance user acceptance testing (UAT). Upon completion of testing, DNR authorizes the TPSO to move the change into the production environment. DNR conducts post-implementation review to verify the change meets user expectations.

MiConnect changes generally consist of system upgrades, hunting and fishing regulation updates, and the correction of programming errors.

AUDIT OBJECTIVE

To assess the sufficiency of DNR's efforts to implement change controls* over the MiConnect application and data.

CONCLUSION

Sufficient, with exceptions.

FACTORS IMPACTING CONCLUSION

- DNR established and implemented the change management procedures and workflow in accordance with State policies, standards, and procedures.
- DNR appropriately implemented some controls over the application in accordance with State policies, standards, and procedures.
- One reportable condition related to maintaining documentation of control activities during the change management life cycle (Finding 4).

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

FINDING 4

Improvements needed to document change control activities.

DNR did not maintain documentation of control activities performed during the change management life cycle to help ensure all changes to MiConnect were properly tested, implemented, and reviewed.

SOM Technical Procedure 1340.00.060.04.01 requires each test type (e.g., UAT) to have its own documentation. Also, the procedure requires the agency business owner to have an authorized tester perform and document UAT and perform application validation to ensure changes were applied and function as expected.

Testing documentation is required for the initiation, construction, testing, implementation, and closeout steps. All steps are required to be performed for State application, database, and data changes, including vendor supported (COTS products), unless indicated otherwise.

We reviewed 44 MiConnect changes completed from October 1, 2023 through September 30, 2025 and noted DNR did not:

a. Document its approval of the requirements for 31 (70%) changes prior to starting development. SOM technical procedure states the agency business owner is to sign off on the business requirements prior to development.

b. Maintain documentation of UAT for all 44 changes. UAT helps verify system changes are working as intended and reduces any unintended consequences prior to production implementation. Although the UAT approvals generally occurred and moved the change forward in the workflow, maintaining documented UAT results provides details of potential defects and the steps to reproduce testing for post-implementation review.

Documentation was not maintained to support testing for all sampled changes.

c. Maintain documentation of post-implementation validation for all 44 changes. Post-implementation validation helps ensure production changes are applied and function as intended. Maintaining documented results of post-implementation validation produces audit trails of the application changes.

Strong change management controls protect the integrity of the environment by planning, documenting, and approving changes. This can prevent adverse effects on IT services.

DNR misunderstood its responsibilities regarding change management approvals and testing documentation.

RECOMMENDATION

We recommend DNR maintain documentation of control activities performed during the change management life cycle.

AGENCY PRELIMINARY RESPONSE

DNR provided us with the following response:

DNR agrees with the recommendation. DNR will work closely with the vendor to implement the necessary process and system changes to ensure that documentation is maintained for all control activities.

INTERFACE CONTROLS

BACKGROUND

Interface controls ensure the accurate, complete, and timely processing of data exchanged between information systems.

MiConnect interfaces with the Michigan Cashiering and Receivable System (MiCaRS) to record the revenue collected from the sales of hunting, fishing, and recreational licenses. MiCaRS interfaces MiConnect revenue to the State's accounting system — Statewide Integrated Governmental Management Applications* (SIGMA). In fiscal years 2024 and 2025, DNR informed us the interface between MiConnect and MiCaRS processed $79.7 and $86.4 million in revenue, respectively.

The Accounting Services Division (ASD) performs daily reconciliations to ensure all MiConnect revenue is transferred accurately and completely to MiCaRS.

AUDIT OBJECTIVE

To assess the effectiveness of DNR's interface controls over MiConnect.

CONCLUSION

Effective.

FACTORS IMPACTING CONCLUSION

- DNR established and implemented interface policies, procedures, and strategies that generally complied with industry best practices.
- For 100% of the batch interface dates reviewed, MiConnect data successfully transferred all revenue transactions to MiCaRS.
- MiConnect revenues materially reconciled with revenues recorded in SIGMA.
- DNR reviewed and corrected all interface processing errors in a timely manner.

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

SYSTEM DESCRIPTION

In October 2018 DNR contracted with a TPSO for MiConnect, an externally hosted, COTS product for the sale and purchase of hunting, fishing, snowmobile, and off-road vehicle licenses. Also, MiConnect is used for hunting lottery applications, fuelwood permits, signing up for Outdoor Skills Academy classes (e.g., fishing clinics, hunting clinics, and survival classes), and deer harvest patches. The application is used by 3,947 State, vendor, and authorized retail users.

Customers can purchase various hunting, fishing, and recreational licenses via the Internet or at an authorized retailer. For fiscal years 2024 and 2025, DNR informed us 2.3 million and 2.4 million transactions were processed totaling $79.7 million and $86.4 million, respectively.

AUDIT SCOPE, METHODOLOGY, AND OTHER INFORMATION

AUDIT SCOPE

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

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

PERIOD

Our audit procedures, which included a preliminary survey, audit fieldwork, report preparation, analysis of agency responses, and quality assurance, generally covered October 1, 2023 through September 30, 2025.

METHODOLOGY

We conducted a preliminary survey to gain an understanding of DNR's IT systems to establish our audit objectives, scope, and methodology. During our preliminary survey, we:

- Interviewed DNR management to obtain an understanding of all DNR IT systems.
- Reviewed SOM policies and procedures related to security and access controls.
- Obtained an understanding of DNR's key processes, systems, and internal control significant to the potential audit objectives.
- Interviewed DNR management and staff responsible for administering and securing MiConnect.
- Reviewed Natural Resources Commission meeting minutes from October 2023 through August 2025.

OBJECTIVE 1

To assess the effectiveness of DNR's security and user access controls over the MiConnect application and data.

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

To accomplish this objective, we:

- Interviewed DNR management and staff to obtain an understanding of its implemented security and access controls.
- Tested select security configurations against State policy and industry best practices.
- Reviewed DNR policies to obtain an understanding of segregation of duties and reviewed all users assigned multiple roles to determine if they were assigned incompatible roles in MiConnect.
- Reviewed last log-in dates for all 3,921 active MiConnect accounts as of July 30, 2025 to verify user accounts were disabled after 60 days of inactivity.
- Randomly and judgmentally sampled 22 of 153 internal users who obtained access from October 1, 2023 to July 30, 2025 to determine if DNR granted access according to SOM technical standards.
- Randomly and judgmentally sampled 39 of 541 internal user accounts which were created prior to July 31, 2024 to determine if DNR recertified users according to SOM technical standards.
- Randomly and judgmentally sampled 12 of 61 internal users whose access was disabled from October 1, 2023 to July 30, 2025 to determine if DNR removed terminated users in a timely manner according to SOM technical standards.
- Reviewed and tested the role permissions for all read-only user roles to validate the users could not edit MiConnect data.
- Performed an analytical review of authorized agents to determine if they met the minimum required annual sales revenue to remain an agent.

Our random samples were selected to eliminate any bias and enable us to project the results to the respective populations. Our judgmental samples were selected based on risk and to ensure significant State government operations within the population were sufficiently reviewed. For our judgmental samples, we could not project the results to the respective populations.

OBJECTIVE 2

To assess the sufficiency of DNR's monitoring efforts of MiConnect's TPSOs.

To accomplish this objective, we:

- Obtained and examined the MiConnect TPSO's SOC reports covering the periods from July 1, 2023 through June 30, 2024 and July 1, 2024 through June 30, 2025 to:
    - Verify the issuing audit firm was credible and qualified.
    - Verify the scope of the SOC reports were appropriate, including the type, reporting period, and trust services criteria used.
    - Identify subservice organizations and whether the organizations' controls were incorporated into the reports.
- Obtained and examined DNR's review of the TPSO's SOC reports to verify if DNR:
    - Received and completed a review of the SOC reports in the required time frame.
    - Obtained SOC reports for subservice organizations or appropriately documented their rationale to not obtain SOC reports.
    - Obtained a bridge letter to address coverage gaps between the reporting period and the State's fiscal year.
    - Evaluated and documented its review of user entity responsibilities noted within the SOC reports.
    - Evaluated and documented its review of deviations noted in the SOC reports.

OBJECTIVE 3

To assess the sufficiency of DNR's efforts to ensure the completeness and accuracy of data within MiConnect.

To accomplish this objective, we:

- Interviewed DNR management and staff to obtain an understanding of MiConnect and processes related to customer and product data.
- Performed a comparison of select data fields to identify differences between MiConnect and DOS driver's license data.

- Determined customer eligibility according to:
    - Date of birth for senior or youth-discounted hunting and fishing licenses.
    - Date of birth for hunting and fishing licenses restricted to specific age groups.
    - Randomly sampled 33 of 4,482,102 product purchases made between October 1, 2023 and July 25, 2025 to determine the state of residence for discounted hunting and fishing licenses or licenses restricted by residency to ensure customers received the appropriate license based on their state of residence.
- Randomly sampled 33 of 266,599 applicants eligible for lottery-based licenses for which drawings occurred from October 1, 2023 through September 15, 2025.
- Analyzed MiConnect customer data to identify instances where the same driver's license number appeared across multiple unique customer records to determine the existence and number of potentially duplicative customer accounts.
    - Randomly sampled 18 of 176 driver's license numbers associated with multiple unique customer records that purchased a license between October 1, 2023 and July 25, 2025 to review and determine if the accounts were associated with the same customer.
    - For 6 of the 18 sampled driver's license numbers, we determined the duplicate accounts were associated with the same customer and reviewed purchases associated with duplicated accounts to determine if customers circumvented license limits.
- Randomly sampled 33 of 4,110 potentially duplicative customer records that purchased a license between October 1, 2023 and July 25, 2025, where the same first and last name and date of birth appeared across multiple unique customer records, to determine if there is a match between the customers' records.
- Reviewed purchases by customers with an active revocation from October 1, 2023 through August 19, 2025 to determine if MiConnect prevented a new purchase during the revocation period.

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

OBJECTIVE 4

To assess the sufficiency of DNR's efforts to implement change controls over the MiConnect application and data.

To accomplish this objective, we:

- Interviewed DNR management and staff to obtain an understanding of MiConnect and the processes related to change controls.
- Randomly sampled 44 changes implemented in MiConnect from October 1, 2023 through September 30, 2025. Those included 34 of 418 changes from project (a) and 10 of 99 changes from project (b) implemented in MiConnect and tested for compliance with the State's change management policies and procedures.

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

OBJECTIVE 5

To assess the effectiveness of DNR's interface controls over MiConnect.

To accomplish this objective, we:

- Obtained an understanding of the population of MiConnect interfaces and judgmentally selected and reviewed one of 22 interfaces as of July 22, 2025 to:
    - Review interface documents for compliance with industry best practices.
    - Randomly sample 33 of 670 batch interface dates from October 1, 2023 through July 31, 2025 and validate the files were successfully transferred, appropriately reconcilied, and errors handled according to procedures.
- Reconciled the revenue recorded in MiConnect and MiCaRS from October 1, 2023 to June 30, 2025 with the corresponding recorded SIGMA revenue.

Our random samples were selected to eliminate any bias and enable us to project the results to the respective populations. Our judgmental samples were selected based on risk and to ensure significant State government operations within the population were sufficiently reviewed. For our judgmental samples, we could not project the results to the respective populations.

CONCLUSIONS

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

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

CONFIDENTIAL AND SENSITIVE INFORMATION

Because of the confidentiality of MiConnect customer and financial data, security and access controls, and user entity responsibilities, we summarized our testing results for presentation in the report and provided the underlying details to DNR's management.

AGENCY RESPONSES

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

The agency preliminary response following each recommendation in our report was taken from the agency's written comments and oral discussion at the end of our fieldwork. Section 18.1462 of the *Michigan Compiled Laws* requires an audited agency to develop a plan to comply with the recommendations and submit it to SBO upon audit completion. The State of Michigan Financial Management Guide (Part VII, Chapter 3, Section 100) requires the audited agency to develop the plan as early as practicable and within 60 days after report issuance and submit the plan to OIAS, SBO. Within 30 days of receipt, OIAS will 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 protecting data from unauthorized modification, loss, or disclosure by restricting access and detecting inappropriate access attempts.
ASD	Accounting Services Division.
availability	Timely and reliable access to data and information systems.
change controls	Controls ensuring program, system, or infrastructure modifications are properly authorized, tested, documented, and monitored.
commercial-off-the-shelf (COTS)	Hardware or software IT products that are ready-made and available for purchase by the general public.
confidentiality	Protection of data from unauthorized disclosure.
DNR	Department of Natural Resources.
DOS	Department of State.
DTMB	Department of Technology, Management, and Budget.
effectiveness	Success in achieving mission and goals.
FISCAM	Federal Information System Controls Audit Manual.
integrity	Accuracy, completeness, and timeliness of data in an information system.
internal control	The plan, policies, methods, and procedures adopted by management to meet its mission, strategic plan, 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, in the auditor's judgment, which 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.
MiCaRS	Michigan Cashiering and Receivable System.
National Institute of Standards and Technology (NIST)	An agency of the U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs.
OIAS	Office of Internal Audit Services.
performance audit	An audit which 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.
personally identifiable information (PII)	Any information about an individual maintained by an agency with respect to, but not limited to: education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual's identity (e.g., name, social security number, date and place of birth, mother's maiden name, biometric records) including other personal information linked or linkable to an individual.
POS	point-of-sale.
principle of least privilege	The practice of limiting access to the minimal level which will allow normal functioning. Applied to employees, the principle of least privilege translates to giving people the lowest level of user access rights they can have and still do their jobs. The principle is also applied to things other than people, including programs and processes.
privileged users	A user that is authorized — and therefore, trusted — to perform security-relevant functions that ordinary users are not authorized to perform.

products	Items or services available to purchase within MiConnect include hunting, fishing, snowmobile, off-road vehicle licenses, hunting lottery applications, fuelwood permits, and Outdoor Skills Academy classes (e.g., fishing clinics, hunting clinics, survival classes, etc.).
reportable condition	A matter, in the auditor's judgment, 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.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
segregation of duties	Separation of the management or execution of certain duties or areas of responsibility to prevent or reduce opportunities for unauthorized modification or misuse of data or service.
SOM	State of Michigan.
State of Michigan Financial Management Guide (FMG)	A consolidation of State financial management policies and procedures.
Statewide Integrated Governmental Management Applications (SIGMA)	The State's enterprise resource planning business process and software implementation suite supporting budgeting, accounting, purchasing, human resource management, and other financial management activities.
System and Organization Controls (SOC) report	Designed to help organizations providing services to user entities build trust and confidence in their delivery processes and controls through a report by an independent certified public accountant (CPA). Each type of SOC report is designed to meet specific user needs: • SOC 1 (Report on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting) - Intended for user entities and the CPAs auditing their financial statements in evaluating the effect of the service organization's controls on the user entities' financial statements. • SOC 2 (Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy) - Intended for a broad range of users needing information and assurance about a service organization's controls relevant to any combination of the five predefined control principles.

There are two types of SOC 1 and SOC 2 reports:

  - Type 1 - Reports on the fairness of management's description of a service organization's system and the suitability of the design of the controls to achieve the related control objectives included in the description, as of a specified date.

  - Type 2 - Includes the information in a type 1 report and also addresses the operating effectiveness of the controls to achieve the related control objectives included in the description, throughout a specified period.

- SOC 3 (Trust Services Report for a Service Organization) - Intended for those needing assurance about a service organization's controls affecting the security, availability, or processing integrity of the systems a service organization employs to process user entities' information, or the confidentiality or privacy of information, but not having the need for or the knowledge necessary to make effective use of a SOC 2 report.

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

TPSO third-party service organization.

UAT user acceptance testing.

user entity responsibility Responsibilities necessary for the user entity to derive the intended benefits of using the services of the service organization.

This Page Left Intentionally Blank

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