STATE OF MICHIGAN
DEPARTMENT OF STATE POLICE
LANSING

GRETCHEN WHITMER
GOVERNOR

COL. JAMES F. GRADY II
DIRECTOR

February 20, 2026

Ms. Jessica Thomas
Chief Internal Auditor
Office of Internal Audit Services
State Budget Office
111 South Capitol Avenue
Seventh Floor, Romney Building
Lansing, Michigan 48933

Dear Ms. Jessica Thomas,

In accordance with the State of Michigan, Financial Management Guide, Part VII, enclosed is our final corrective action plan to address recommendations contained within the Office of the Auditor General report of the Michigan Department of State Police Michigan Sex Offender Registries:

If you have any questions regarding the corrective action plan, please feel free to contact me.

Sincerely,

Amanda J. Baker
Internal Control Officer and Division Director
Budget, Financial, and Facilities Division

Enclosure
cc: Executive Office
Office of the Auditor General
House Fiscal Agency
Senate Fiscal Agency
House Appropriations Committee
Senate Appropriations Committee
Col. James F. Grady II
Lt. Col. Aimee Brimacombe
F/Lt. Roger Hunt
Melissa Castro
Michelle Kleckler

Michigan Department of State Police (MSP)
Michigan Sex Offender Registries (551-0595-24)
Issued By Office of the Auditor General (OAG)
October 16, 2025
Department Final Corrective Action Plan

Summary Response Matrix

	Complied	Will Comply	Partially Complied	Will Not Comply
Agrees	4	1, 2, 3, 5		
Partially Agrees				
Disagrees				

Final Corrective Action Plan (CAP)

Finding Number 1: Monitoring improvements needed for Third Party Service Organization (TPSO).

Related IT system, if applicable: Michigan Sex Offender Registry (MSOR) and the Public Sex Offender Registry.

Recommendation: We recommend MSP improve its monitoring of MSOR's TPSO.

Department Response/Management Views: MSP agrees and will comply.

Planned Corrective action steps that will be implemented: The Sex Offender Registry (SOR) Unit manager added calendar reminders to follow-up with the vendor to obtain the Systems and Organization Controls (SOC) report once it is complete. The vendor anticipates receiving the completed SOC report for the period of April 1, 2023, through March 31, 2024, in December 2025. The SOR Unit manager will monitor the vendor for contractual compliance of obtaining and reviewing the subservice organization SOC report. *Anticipated Completion Date – March 31, 2026.*

Information Technology Operations Section analyst will create a process map for obtaining SOC 2 reports that will be reviewed and approved by IT Operations Section manager. *Completed – February 3, 2026.*

Information Technology Operations Section specialist will develop procedures for obtaining and reviewing the SOC 2 report and communicate procedures to Information System Owners. These procedures will include how compliance with the procedures will be monitored and will be reviewed annually by IT Operations Section data privacy specialist or manager. *Anticipated Completion Date – March 31, 2026.*

Information Technology Operations Section data privacy specialist and manager will determine what database or workflow tool to use for tracking and sending notifications to business owners 90-days prior to SOC 2 report expiration dates. The notifications will remind Information System Owners to request the SOC 2 report from vendors timely. Once a notification tool is selected, the Information Technology Operations Section manager will communicate the new process to applicable Information System Owners. *Anticipated Completion Date – February 28, 2026.*

Information Technology Division (ITD) will work with business owners and Department of Technology, Management and Budget (DTMB) - Agency Services in collaboration with the vendor on the design, implementation, and monitoring of Complementary User Entity Controls. MSP will continue working with DTMB Office of Internal Audit Services to better understand SOC related guidance in the Financial Management Guide. *Anticipated Completion Date – July 1, 2026.*

Overall Anticipated Compliance Date: 07/01/2026.

MSP Responsible Individuals: Capt. Matt Bolger, ITD Director and Michelle Kleckler, Criminal Justice Information Center (CJIC) Division Director.

Finding Number 2: Security and access controls over MSOR need improvement.

Related information system, if applicable: MSOR, the Public Sex Offender Registry, Michigan Criminal Justice Information Network (MiCJIN), MSP Active Directory (MSPAD).

Recommendation: We recommend MSP improve security and access controls over MSOR to help prevent unauthorized access, disclosure, modification, or destruction of Criminal Justice Information (CJI).

Department Response/Management Views: MSP agrees with this recommendation and is working to implement the corrective actions detailed below.

Planned Corrective action steps that will be implemented:

Milestone 1: Consistently perform effective user account management.
Key process enhancements following the implementation of a Lean Process Improvement (LPI) will include:

Section a.
Subsection 1.

- Authorization request forms exist for MSP users; MSP will develop an authorization request form for access to MSOR and all MiCJIN applications for non-MSP State of Michigan (SOM) users and local agency users specifying application user level access. Please reference milestone 2 for information on monitoring the access rights. Responsible individual: Tara Smith, Access and Control Unit Manager. *Anticipated completion date – October 31, 2026.*
- MSP will retrain access control unit members to ensure the access granted reflects the access approved on the access authorization forms. *Completed – November 25, 2025.*
- MSP will generate a notification that is sent to the user and the user's manager and the information system owner notifying the specific role-based access that is granted to the user at the time access is granted. *Anticipated completion date – October 31, 2026.*
- MSP will require DTMB to establish an authorization form. Responsible individuals: Michelle Kleckler, CJIC Division Director and Eric Fowler, Data Strategy and Governance Section Manager. *Anticipated completion date – March 30, 2026.*

Subsection 2.

- MSP will add a checkbox to the authorization request form for the authorized requestor to confirm fingerprint-based background check compliance. Responsible individual: Tara Smith, Access and Control Unit Manager. *Anticipated completion date – October 31, 2026.*
- Criminal Justice Information Services (CJIS) Compliance Auditors will continue to review and verify compliance with CJIS fingerprint-based background check requirements for access to applications that access or contain CJI.
- Beginning in 2006, fingerprints collected as the result of a background check for the purposes of criminal justice employment and criminal justice information access are retained in the criminal history repository. Prior to 2006, these fingerprints were not retained.

Subsection 3.

- MSP will add a checkbox to the authorization request form for the authorized requestor to confirm CJIS security and privacy training compliance. Responsible individual: Tara Smith, Access and Control Unit Manager. *Anticipated completion date – October 31, 2026.*
- CJIS Compliance Auditors will continue to review and verify compliance with CJIS security and privacy training requirements for access to applications that access or contain CJI.
- CJIC staff has employed an automated mechanism that sends reminder emails to individual users 60, 30, 5, and 1 day(s) prior to CJIS security and privacy training expiration.

Subsection 4.

- MSP will add a checkbox to the authorization request form for the authorized requestor to confirm Law Enforcement Information Network (LEIN) training compliance. Responsible individual: Tara Smith, Access and Control Unit Manager. *Anticipated compliance date – October 31, 2026.*
- CJIS Compliance Auditors will continue to review and verify compliance with LEIN training and certification requirements for access to applications that access LEIN.
- CJIC staff have employed a monthly process of monitoring LEIN certification expiration dates and sending email reminders to agencies who are expired or approaching their expiration.

Section b.

Subsection 1.

- MSP will request an ETRB exception to not disable user access if the user has not accessed the application for enforcement reasons within a specific timeframe due to the nature of the position. The ETRB exception will specifically list every application that is relevant to the exception. Currently, notifications are sent manually via email to each information system owner, as each system requires a different process for disabling, removing, or wiping accounts. If an Application Programming Interface (API) integration becomes available in the future, the process will be automated. Responsible individuals: Michelle Kleckler, CJIC Division Director, and Eric Fowler, Data Strategy and Governance Section Manager. *Anticipated completion date – July 31, 2026.*
- MSP will perform annual user recertifications of non-privileged and privileged user access rights to ensure MSOR SOM users who have been inactive for more than 60 days still meet the requirements of the above exception condition, otherwise access will be removed. Responsible individual: Tara Smith, Access and Controls Unit Manager. *Anticipated completion date – April 30, 2026.*

Subsection 2.

- MSP will request an ETRB exception to not disable user access if the user has not accessed the application for enforcement reasons within a specific timeframe due to the nature of the position. The ETRB exception will specifically list every application that is relevant to the exception. Currently, notifications are sent manually via email to each information system owner, as each system requires a different process for disabling, removing, or wiping accounts. If an API integration becomes available in the future, the process will be automated. Responsible individuals: Michelle Kleckler, CJIC Division Director, and Eric Fowler, Data Strategy and Governance Section Manager. *Anticipated completion date – July 31, 2026.*
- MSP will perform annual user recertifications of non-privileged and privileged user access rights to ensure MSOR non-SOM users who have been inactive for more than 97 days still meet the requirements of the above exception condition, otherwise access will be removed. Responsible individual: Tara Smith, Access and Controls Unit Manager. *Anticipated completion date – April 30, 2026.*

Section c.

- MSP will add disabled user accounts to the driver to automatically disable user access at the application level in MiCJIN when a user's work site or email address is removed in MSPAD and a user's network account is disabled. MSOR becomes inaccessible once network access is removed, and communication via e-mail is sent to the information system owner to manually remove access. *Anticipated Completion Date – December 1, 2026.*
- MSP will add disabled user accounts to the driver to automatically disable user access at the application level in MiCJIN when a local agency administrator disables a user's account in AdminTool. MSOR becomes inaccessible once network access is removed, and communication via e-mail is sent to the information system owner to manually remove access. *Anticipated Completion Date – December 1, 2026.*
- MSP will implement a process whereby information system owners, including MSOR, will be notified when a user of their information system has had their access revoked. MSP will make business owners responsible for ensuring application-level (backend) accounts have been disabled in their information systems. *Anticipated Completion Date – December 1, 2026.*
    - MSOR has updated system configurations to allow user access removal at the application level. *Completed – November 30, 2025.*
    - MSOR will work with Information Technology Division, Security and Network Unit teams to develop and finalize user access removal processes. Until an automatic removal is possible, manual emails will be sent in the interim to notify business owners that a user's access requires removal. *Anticipated Completion Date – March 1, 2026.*

Milestone 2: Account Verifications and modifications.
Key process enhancements following the implementation of a LPI will include:

Section d.
Subsection 1.

- MSP will automate the annual recertifications of non-privileged user access rights within MiCJIN. Responsible individual: Tara Smith, Access and Controls Unit Manager. *Completed – December 11, 2025.*
- MSP will maintain documentation to support which users were verified, who completed the verification, and the dates of the verification. Responsible individual: Tara Smith, Access and Controls Unit Manager. *Anticipated Completion Date – March 2, 2026.*
- MSP will retrain recertification staff to ensure that the DTMB Access Control Standard is followed. Responsible individual: Tara Smith, Access and Controls Unit Manager. *Completed – December 11, 2025.*

Subsection 2.

- The 2025 DTMB IT update to 1340.00.020.01 Access Control Standard changed the privileged user review requirements from semi-annual to annual, subsequent to the Michigan Sex Offender Registries audit. MSP will automate the annual recertifications of privileged user access rights within MiCJIN. Responsible individual: Tara Smith, Access & Controls Unit Manager. *Completed – December 11, 2025.*
- MSP will maintain documentation to support which users were verified and who completed the verification and the dates of the verification. Responsible individual: Tara Smith, Access & Controls Unit Manager. *Anticipated Completion Date – March 2, 2026.*
- MSP will retrain recertification staff to ensure that the DTMB Access Control Standard is followed. Responsible individual: Tara Smith, Access & Controls Unit Manager. *Completed – December 11, 2025.*

Milestone 3: Ensure appropriate security configurations.
Key process enhancements following the implementation of a LPI will include:

- MSP will take the necessary steps to ensure that security configurations for MiCJIN, MSPAD, and MSOR are properly implemented and regularly reviewed for appropriateness. Because of the confidentiality of these security configurations, MSP provided the details to Office of Internal Audit Services.

Overall Anticipated Compliance Date: July 31, 2026

MSP Responsible Individuals: Capt. Matt Bolger, ITD Director and Michelle Kleckler, CJIC Division Director.

Finding Number 3: Additional training and guidance needed to ensure validity, accuracy, and completeness of MSOR records.

Related IT system, if applicable: MSOR and the Public Sex Offender Registry.

Recommendation: MSP should improve the training and guidance to registering authorities for registering and updating sex offender's information to help ensure the validity, accuracy, and completeness of MSOR records.

Department Response/Management Views: MSP agrees and will comply.

Planned corrective action steps that will be implemented: SOR unit Subject Matter Experts (SMEs) reinstituted trainings to local registering authorities during summer 2025. Trainings are being scheduled through 2026. The SOR unit manager monitors that training occurs by requiring prior registration for in-person training through MiTrain or the Professional Development Learning Center (PDLC) and reviewing attendance lists from virtual trainings. The training curriculum is reviewed and updated periodically by the SOR unit manager and staff as training needs are identified and when enhancements are made to the MSOR system. This curriculum covered both the use of the system and the appropriate guidelines for its utilization to support local law enforcement agencies. While MSP maintains the database, it is the responsibility of local law enforcement agencies to accurately and completely input registrant information. The SOR unit staff monitors certain data element errors during the course of their normal job duties and monitors for improvements for future training needs. Training courses are also available on the MiCJIN Community Page. The approval of the 2023 SMART Grant provided funding for the areas of continued training, staff resources, and data correction. The need for additional guidance was originally recognized in FY 2022, prior to the audit, with the SMART grant submission request for training. The SMART grant was submitted and approved under FY 2023. *Anticipated Completion Date – September 30, 2026.*

Comment on CAP from Michigan Office of the Auditor General (03/20/2026, 10:00 AM)
This information was not provided during our audit fieldwork. Therefore, the OAG did not validate or conclude on this information.

Overall Anticipated Compliance Date: September 30, 2026, and ongoing thereafter.

Responsible Individual: F/Lt. Roger Hunt, CJIC Incident Section Manager.

Finding Number 4: Documentation not maintained to support registrants who are no longer living in Michigan.

Related IT system, if applicable: MSOR and the Public Sex Offender Registry.

Recommendation: MSP should improve its process for maintaining appropriate documentation for registrants who are no longer domiciled, temporarily residing, working, or attending school within Michigan.

Department Response/Management Views: MSP agrees and has complied.

Corrective action steps that have been implemented: During the audit, documents to support registry removal were researched. Missing documents were added to the records. *Completed – June 13, 2025.*

During a SOR Unit meeting, the SOR Unit Manager emphasized to SOR unit staff the requirement to add supporting documentation to records to support the offender status being changed to out-of-state status. SOR unit analyst will review quarterly a sample of pending out-of-state records for appropriate uploaded documentation. *Completed – October 21, 2025.*

Overall Compliance Date: October 21, 2025.

Responsible Individual: F/Lt. Roger Hunt, CJIC Incident Section Manager.

Finding Number 5: Improved guidance needed for identification of registrants who missed address verifications.

Related IT system, if applicable: MSOR and the Public Sex Offender Registry.

Recommendation: We recommend MSP improve its guidance to registering authorities to identify when registrants fail to verify their address.

Department Response/Management Views: MSP agrees and will comply.

Planned corrective action steps that will be implemented: SOR unit SMEs reinstituted trainings to local registering authorities during Summer 2025. Trainings are being scheduled through 2026. The SOR unit manager monitors that training occurs by requiring prior registration for in-person training through MiTrain or the PDLC and reviewing attendance lists from virtual trainings. The training curriculum is reviewed and updated periodically by the SOR unit manager and staff as training needs are identified and when enhancements are made to the MSOR system. This curriculum covered both the use of the system and the appropriate guidelines for its utilization to support local law enforcement agencies. While MSP maintains the database, it is the responsibility of local law enforcement agencies to monitor active registrants. The SOR unit staff monitors errors during the course of their normal job duties and monitors for improvements for future training needs. Training courses are also available on the MiCJIN Community Page. The approval of the 2023 SMART Grant has provided funding for the areas of continued training, staff resources, and data correction. The need for additional guidance was originally recognized in FY 2022, prior to the audit, with the SMART grant submission request for training. The SMART grant was submitted and approved under FY 2023. *Anticipated Completion Date – September 30, 2026.*

Overall Anticipated Compliance Date: September 30, 2026, and ongoing thereafter.

Responsible Individual: F/Lt. Roger Hunt, CJIC Incident Section Manager.

Comment on CAP from Michigan Office of the Auditor General (03/20/2026, 10:00 AM)

During the audit, the OAG validated 3 offenders having complete documentation in MSOR, however, one offender noted in the finding did not.

Comment on CAP from Michigan Office of the Auditor General (03/20/2026, 10:00 AM)

This information was not provided during our audit fieldwork. Therefore, the OAG did not validate or conclude on this information.