MNDRIVE Systems Audit Report 2025

The Minnesota Legislature, under Minnesota Statute 171.12, Subdivision 1a, established requirements the Department of Public Safety's (DPS) Driver and Vehicle Services (DVS) division must adhere to regarding the access and integrity of private data within the DVS information system known as MNDRIVE. DPS has been mandated to conduct independent audits of these requirements on a biennial basis.

DPS hired Berry, Dunn, McNeil & Parker, LLC (BerryDunn) to satisfy this mandate in early 2025. The audit was designed to assess DVS's management of the MNDRIVE system and DVS' compliance with the requirements of Minnesota Statute 171.12 Subdivision 1a. The audit concluded on June 30, 2025.

The four audit objectives:

1. DVS established access control procedures and used them to assess whether individuals authorized by law can enter, update or access non-public data and that an individual's access corresponds to their official duties. This is a requirement in Minnesota Statute 171.12, Subdivision 1a(a.)
2. MNDRIVE maintains a data audit trail where all queries and responses as well as all actions in which data is entered, updated, accessed, shared or disseminated are recorded. This is a requirement in Minnesota Statute 171.12, Subdivision 1a(a).
3. If DVS determines an individual willfully entered, updated, accessed, shared or disseminated data in violation of state or federal law, DVS must impose disciplinary action as directed by the commissioner of public safety. If an individual willfully gained access to data without authorization by law, the division refers the matter to the appropriate prosecuting authority. This is a requirement in Minnesota Statute 171.12, Subdivision 1a(b).
4. The commissioner and division have an established process that allows an individual who was subject to disciplinary action to appeal the action. The division notifies the individuals subject to disciplinary action in writing of the action, explains the reason for the action and explains how to appeal the action. DVS must transmit the notification within five calendar days of the action. 171.12, Subdivision 1a(c)

Overall findings

BerryDunn found deficiencies in three of the four objectives.

Objective No. 1

The procedures performed identified one deficiency related to policy and availability of supporting documentation related to management and authorization of users' MNDRIVE system access, reported as Finding 2025-1.

Objective No. 2

The procedures performed identified one deficiency related to the creation and review of audit reports within MNDRIVE, reported as Finding 2025-2.

Objective No. 3

The procedures performed did not identify any deficiencies related to DVS' operation and management of the MNDRIVE system for this objective.

Objective No. 4

The procedures performed identified one deficiency related to the policy detailing the employee's appeal rights when disciplinary action is necessary, reported as Finding 2025-3.

Corrective actions

DVS acknowledges each of these audit findings and appreciates the recommendations provided by BerryDunn. Work has begun to proactively address these deficiencies.

The Department of Public Safety is committed to upholding the highest standards of data security, oversight and compliance. These audit findings and accompanying recommendations provide an opportunity to improve internal policies, strengthen procedures and ensure continuous improvement of our systems.

In response to the audit findings, DVS developed the following corrective actions:

Objective No. 1

Prior to the audit, DVS had Identity Access Management personnel actively addressing security standards for the MNDRIVE system. Developing permissions relational to relevant roles is an ongoing process. Indexing of permissions appropriate for user roles is currently happening through an existing security access application process.

Permission assignments should be standardized in policy and procedure. Finding 2025-1 found that currently they are not standardized. The policies DVS is developing will emphasize role-based access controls which align with a user's official job duties and required training. Scheduled review and recertification of access rights will be included in these policies.

BerryDunn further found that while Security Access applications are collected and reviewed by DVS staff, Minnesota IT Services (MNIT) staff grant permissions in the system. Documentation in the form of a joint powers agreement or intra-agency agreement outlining the responsibilities and roles of each of these entities could not be produced. DVS will investigate current processes while developing the permissions policies. It will also confirm if permissions granting appropriate responsibilities lie with MNIT and if so, will develop an agreement with MNIT to document those responsibilities.

DVS expects this objective to be completed by the end of fiscal year 2026 (FY26). Access management will be a continuous improvement initiative.

Objective No. 2

DVS is compliant with Objective No. 2 because MNDRIVE has been built to create a data audit trail for each user's actions within the system. DVS is proactively discovering system misuse and successfully enforcing discipline action. BerryDunn identified opportunities for DVS to potentially do more of this work by effectively leveraging reporting functions.

Finding 2025-2 concerns DVS' reporting and auditing of the MNDRIVE system. DVS provided a list of reports built within MNDRIVE that capture auditable events. DVS is actively working through and closing out open audits following established policy and procedures relating to MNDRIVE misuse. Primary findings are expected to be resolved by the end of FY26. DVS proactively enforces eServices self-searching to prevent accessing account information or reports for personal use. Cases of misuse are being proactively identified and dealt with through disciplinary action. Access management will be a continuous improvement initiative.

Finding 2025-2 also indicates there are reports built within the system that are not being systematically ran and analyzed. DVS intends, as the system matures and to the degree resources allow, to pursue all reasonable actions to maintain security and integrity of the information housed in MNDRIVE. Some of the reports built while the system was stood up have little value, and others require many hours of analysis to be fruitful.

In response to this finding, within the next 12 months, DVS Data Services staff will formally review the full inventory of reports relating to auditable events. DVS will:

- Identify the most relevant reports.
- Establish procedures and schedules for relevant reports.
- Remove irrelevant reports from the system.

Objective No. 4

Objective No. 4 evaluated DVS policies and procedures supporting appeals rights for MNDRIVE users who were subject to disciplinary actions following misuse of the system.

Finding 2025-3 identified an inconsistency in DVS policy. DVS Policy 00-22, Revision 0.0, dated Feb. 9, 2022, erroneously states, "If the auditor determines misuse occurred, those findings are final and your access to DVS information systems will be immediately and permanently revoked. You will have no opportunity to appeal the auditor's decision within the Department of Public Safety."

DVS failed to update Policy 00-22 when due process provisions were added to Minnesota Statute 171.12. This policy has been updated since the BerryDunn audit and Revision 1.0 is in the final stages of review before publication, which is expected by Sept. 30, 2025.

Conclusion

The 2025 MNDRIVE systems audit identified deficiencies in three of four audited objectives. These specifically related to user access management, reporting and audit trail review, and due process policies around disciplinary actions. While these findings point to areas for improvement, they also affirm that foundational elements of security, compliance and data accountability are in place, particularly regarding enforcement of system misuse (objective No. 3). DVS currently reviews system access requests and assigns permissions relevant to the roles but needs to develop a more systematic approach to these functions and document in procedure (objective No. 1).

DVS currently does audit system use and proactively identifies system misuse and responds accordingly. However, there are opportunities for DVS to further leverage the system's reporting capabilities (objective No. 2).

BerryDunn's audit findings pinpoint opportunities for DVS to strengthen existing controls. The system is moving out of development and integration stages and into maintenance and enhancement. As the system has matured, so has DVS and its partners' knowledge and abilities in monitoring and administering the system. DVS is committed to addressing the identified issues through the development of corrective actions and the initiation of process improvements.