

Oregon Motor Voter (OMV) Rules Advisory Committee

September 29, 2025



Oregon Administrative Rule

☐ Division 5

☐ VOTER REGISTRATION

☐ 165-005-0170

☐ Oregon Motor Voter Registration

Transferring Data Between DMV and SOS

- Within 5 days of a covered transaction, DMV will make available to SOS, voter registration information for qualified individuals to the SoS.
- Data will be made available to SOS at least once per weekday.
- Electronic records provided by DMV for OMV are classified as Level 4 Restricted.
- Each data transfer will include a notification and count confirmation process.
- Define the process when/If a file is not successfully sent or received.
- The data transfer file prepared by DMV will include the full name, date of birth, residence address, mailing address (if any), date of the DMV interaction, type of DMV interaction, and DMV source of information.
- Define the new monthly OMV file audit process.

Findings Related to this Segment:

Finding 6: *Signature File Transfer Documentation (page 13) Outbound time data for three (3) of thirty-five (35) signature files could not be verified due to unavailable system records, limiting assurance over timely processing.*

Finding 7: *Failure Notification Tracking (page 14) Neither DMV nor SOS maintain formal mechanisms to track and document system-generated failure notifications. Thirteen (13) of fifteen (15) failure notifications provided by SOS were either not resolved timely or lacked sufficient documentation to confirm resolution.*

Finding 8: *User and Admin Access Reviews (page 1) Formal user access reviews are not performed for the OMV system, or for administrative users for MOVEit.*



Information systems included within the scope of this audit testing include:

Administered By	System	Relevant Function
ODOT	Oregon License Issuance and Vehicle Registration (OLIVR)	Processes data for daily DMV credential issuance transactions within field offices, with automated processes to identify eligible individuals for automatic voter registration through the OMV program.
	MOVEit	Secure managed file transfer software used to exchange DMV credential issuance and related OMV program data between DMV and SOS.
	MOVEit Transfer	A component of the MOVEit system, MOVEit Transfer includes the secured FTP site for SOS personnel to access transferred DMV credential issuance and related OMV program data from DMV.
SOS	Oregon Motor Voter System (OMV system)	SOS system with automated job processes receiving and processing DMV credential issuance and related OMV program data.



State of Oregon

Oregon Motor Voter Program Audit

July 1, 2025



6. Incomplete Documentation of Outbound Signature File Transfers

Risk: **Moderate**

Criteria:

- Best practices in data transmission and auditability require that all file transfers, especially those involving sensitive voter registration data be logged, with complete metadata, including timestamps for both inbound and outbound transfers.
- The OMV Program relies on accurate and timely file exchanges between DMV and SOS to ensure voter registration processes are executed in compliance with House Bill 2177.
- Documentation trails must be complete and verifiable to support accountability, enable timely issue resolution, and ensure compliance with legal and operational standards



Cause:

- The ODOT Information Services (IS) team was unable to retrieve transfer time records for the affected dates due to system log retention practices.
- There is no formal policy requiring the consistent capture and retention of outbound transfer metadata.

Effect:

- Lack of available system logs reduce the ability to verify timely processing and successful transmission of voter registration data.
- This gap could hinder compliance verification, delay issue resolution in the event of a dispute or system failure and reduce confidence in the integrity of the OMV Program's data handling processes.



Recommendations:

- 6.1) (ODOT)** Implement a formal logging and retention policy for all OMV-related file transfers, ensuring that both inbound and outbound transfer logs are consistently retained for a sufficient duration for audit purposes.
- 6.2) (ODOT)** Consider enhancing system capabilities or procedures to sufficiently retain outbound transfer logs and metadata for all signature files.
- 6.3) (SoS)** Conduct periodic audits of file transfer logs to ensure completeness and identify any recurring gaps in documentation.



7. Lack of Formal Process for Tracking and Resolving System Failure Notifications

Risk: **Moderate**

Criteria:

- In accordance with the SOS OMV Transfer and Processing Recovery v1.1 procedure (dated July 29, 2021), the following requirements apply to the handling of system-generated failure notifications:
 - Must receive and review all failure notifications by 8:30 AM each business day
 - Logged and tracked in a centralized system
 - Investigated and resolved in a timely manner
 - Supported by documentation evidencing resolution and closeout
- Additionally, guidance from NIST 800-53 emphasizes the importance of:
 - Monitoring and documenting system incidents, including failure notifications
 - Reporting and tracking incidents to ensure appropriate response and resolution
 - Establishing formal procedures for incident handling, including defined roles and responsibilities
 - Reviewing and analyzing system logs to detect and respond to anomalies
- These requirements enable the integrity and reliability of voter registration data transfers between DMV and SOS and help ensure accountability and operational continuity.



Cause:

- Responsibilities for monitoring and resolving system errors are not clearly defined or enforced across agencies.
- There is overreliance on informal communication channels and manual intervention.

Effect:

- System errors may go unresolved or be addressed inconsistently, leading to delays or failures in voter registration data transmission.
 - Incomplete or undocumented resolution processes reduce data integrity and increase the risk of non-compliance with state and federal legislation.
- The absence of a centralized tracking mechanism limits visibility into recurring issues and weakens accountability.



Recommendations:

7.1 (ODOT & SOS) Expand the current centralized failure notification channel to add a consistent mechanism to log, monitor, and document all system-generated errors across both agencies.

7.2 (ODOT & SOS) Develop formal procedures for investigating, resolving, and closing out failure notifications. These procedures should include defined timelines, escalation protocols, and clearly assigned responsibilities.

7.3 (ODOT & SOS) Conduct periodic assessments of failure logs to identify recurring issues, assess resolution timeliness, and implement system improvements.

7.4 (ODOT & SOS) Train relevant staff on the new procedures for investigating, resolving, and closing out failure notifications, and ensure accountability through regular audits and performance monitoring.



8. User Access Reviews Not Performed for Systems Supporting the OMV Program

Risk: **Moderate**

Criteria:

- In accordance with the Oregon Motor Voter law (House Bill 2177, 2015), the Oregon DMV is required to securely transmit sensitive personal information including legal name, date of birth, residence, and citizenship status to the Secretary of State's Elections Division for voter registration purposes.
- Additionally, guidance from NIST 800-53 emphasizes the importance of:
 - Role based access controls that restrict access to authorized personnel only
 - Periodic user access reviews to validate the appropriateness of access rights
 - Timely removal of access for users whose roles no longer require it
- These requirements help to ensure the confidentiality, integrity, and availability of the data and systems supporting the OMV Program.



Cause:

- There is no formalized policy or procedure requiring periodic user access reviews for OMV-related systems.
- Policies and processes for user account management vary across systems, due to various departments or agencies owning/administering systems.
- An additional MOVEit administrative user group was created to align with the updated name for the relevant IT department/group; the original user group was retained out of concern that some users may still require access through it.

Effect:

- Inappropriate user access may persist, increasing the risk of unauthorized access to data and system changes, compromising data integrity and transmission reliability, as information may be altered, corrupted, or fail to transmit in a complete and accurate manner.
- The absence of regular user access reviews and automated controls weakens the overall security posture of the OMV Program.
- Redundant user groups increase the administrative burden and likelihood that access may not be properly managed, potentially resulting in inappropriate access



Recommendations:

8.1 (ODOT) Establish and document a standard formal administrative user evaluation policy for MOVEit and MOVEit Transfer. Assign clear ownership for conducting and documenting periodic access assessments (e.g., quarterly or semi-annually). Implement a centralized tracking mechanism to log user access review dates, findings, and remediation actions.

8.2 (SoS) Establish and document a standard formal user and administrative access evaluation policy for the OMV system. Assign clear ownership for conducting and documenting periodic access assessments (e.g., quarterly or semi-annually). Implement a centralized tracking mechanism to log user access review dates, findings, and remediation actions.

8.3 (ODOT) Remove or consolidate redundant administrative user groups within MOVEit.

8.4 (SoS) Remove unnecessary user roles for the two identified OMV system administrators



Transferring Data Between DMV and SOS

- Within 5 days of a covered transaction, DMV will make available to SOS, voter registration information for qualified individuals to the SoS.
- Data will be made available to SOS at least once per weekday.
- Electronic records provided by DMV for OMV are classified as Level 4 Restricted.
- Each data transfer will include a notification and count confirmation process.
- Define the process when/If a file is not successfully sent or received.
- The data transfer file prepared by DMV will include the full name, date of birth, residence address, mailing address (if any), date of the DMV interaction, type of DMV interaction, and DMV source of information.
- Define the new monthly OMV file audit process.

Next Steps

Next meeting: October 6, 2025

- **Any outstanding File Transfer Between DMV & SOS Items**
- **OMV Processing at SoS**
- **No Meeting October 13th**
- **OMV Processing at SoS Discussion Continues October 20 & 27.**

