Oregon Driver and Motor Vehicle Services Division

Licensing and Registration System Accurately Assesses and Collects Fees, but Security Processes Need Improvement

October 2024

Report 2024-28

Oregon Secretary *of* State
Audits Division

Audit Highlights

Oregon Driver and Motor Vehicle Services Division

Licensing and Registration System Accurately Assesses and Collects Fees but Security Processes Need Improvement

WHY THIS AUDIT IS IMPORTANT

- The Oregon Driver and Motor Vehicle Services Division (DMV) serves over 8,000 people on average each day and 2 million each year.
- The Oregon License Issuance and Vehicle Registration system (OLIVR) uses FAST Enterprises' FastDS-VS® software application for DMV's legacy system replacement from the 1960s.
- Before the implementation of OLIVR in 2019, DMV had only three online services. DMV now offers over 20 online services.
- OLIVR allows for real-time data access, a feature used by many DMV partners, such as law enforcement and vehicle dealerships, which access more than 141,000 records each day.

WHAT WE FOUND

1. OLIVR accurately assesses and collects fees for issuing Oregon drivers licenses and vehicle registrations. (pg. 4)
2. OLIVR accurately and reliably transfers system transaction data into ODOT's main accounting system, the Transportation Environment Accounting and Management System. (pg. 6)
3. While some measures have been taken to help ensure Oregon DMV web content is accessible to persons with disabilities and has appropriate language alternatives for customers who have limited English proficiency, more work still needs to be done to ensure non-English speaking users have access to DMV services through their web portal. (pg. 6)
4. Department management has implemented important protection measures for system security, such as multifactor authentication, system logging, and role-based access, but additional process improvements are needed to better secure the system and its data. Weaknesses included immature processes for granting and reviewing system access, a lack of detailed application security plans, as well as a lack of appropriate periodic security risk assessments. (pg. 7)
5. OLIVR computer code modifications are appropriately controlled to ensure the integrity of the system data is maintained. (pg. 9)

WHAT WE RECOMMEND

We made nine recommendations to the Driver and Motor Vehicle Services Division. The division agreed with all of our recommendations. The response can be found at the end of the report.

Oregon Secretary *of* State
Audits Division

Secretary of State **LaVonne Griffin-Valade**
Audits Director **Kip R. Memmott**

Introduction

The Driver and Motor Vehicle Services Division (DMV) is a large division of the Oregon Department of Transportation (ODOT). DMV works to support ODOT by promoting driver safety, protecting financial and ownership interests in vehicles, and collecting revenues for Oregon's transportation system. DMV is funded entirely by the fees it collects, which include fees for driver licensing, vehicle title and registration, record sales, and fees collected from business licenses, identification cards, and permit testing.

These revenues are collected and accounted for and eventually distributed to designated funds, such as the State Highway Fund, Passenger Rail Account, Parks and Recreation Department, and specialty plate organization recipients. The division's Governor-approved budget for 2023-25 is set at $311 million, with 897 positions and Full-Time Equivalent staffing of 877.

Oregon DMV's customer service is of the highest priority, providing critical transportation services for Oregonians

According to the ODOT DMV Strategic Plan, customer service remains the highest priority and is at the core of DMV's strategic vision. The Field Services department of DMV provides in-person customer service at 59 field offices across Oregon, serving over 8,000 customers each day and over 2 million customer visits per year. Customers are served through processing new driver license applications; administering driver knowledge, skill, and vision tests; issuing photo driver licenses and identification cards; issuing vehicle permits, plates, registration stickers and parking placards for those with disabilities; reinstating driving privileges; and inspecting vehicle identification numbers.

DMV provides services to its customers by issuing more than 550,000 driver licenses and ID cards, 1 million vehicle titles and almost 2 million vehicle registrations each year. DMV offers services via multiple delivery channels, such as in-person, over the phone, through the mail, or online by visiting DMV2U. Passenger vehicle registration is also renewed through partnerships with the Department of Environmental Quality (DEQ) at their emissions testing stations. DMV also regulates and inspects vehicle dealerships, dismantlers and third-party driver testing businesses in Oregon.

Internal and external partners influence DMV's services and how it performs its body of work

DMV serves a large population in Oregon, with this number growing as teenagers and new residents get Oregon identification and driver's licenses, purchase and transfer titles, as well as register for other services provided by DMV. Along with their own set of tasks, DMV partners with many other entities in their daily work. The list of partners is long, and these partnerships can influence how DMV performs its work.

DMV works closely with the Department of Administrative Services' Enterprise Information Services staff, Legislative Fiscal Office, and many other external partners. DMV also interfaces with external partners such as the Secretary of State's Office, Donate Life NW, DEQ, Department of Revenue, cities and counties, and other community partners.

In addition, DMV interfaces with third-party driver testing, Electronic Vehicle Registration, vehicle license plates and registration stickers, specialty plate program, DMV-DEQ interagency support and American

Association of Motor Vehicle Administrators system agreements. The Third-Party Program provides direct oversight of private businesses conducting commercial and non-commercial drive tests on behalf of DMV.

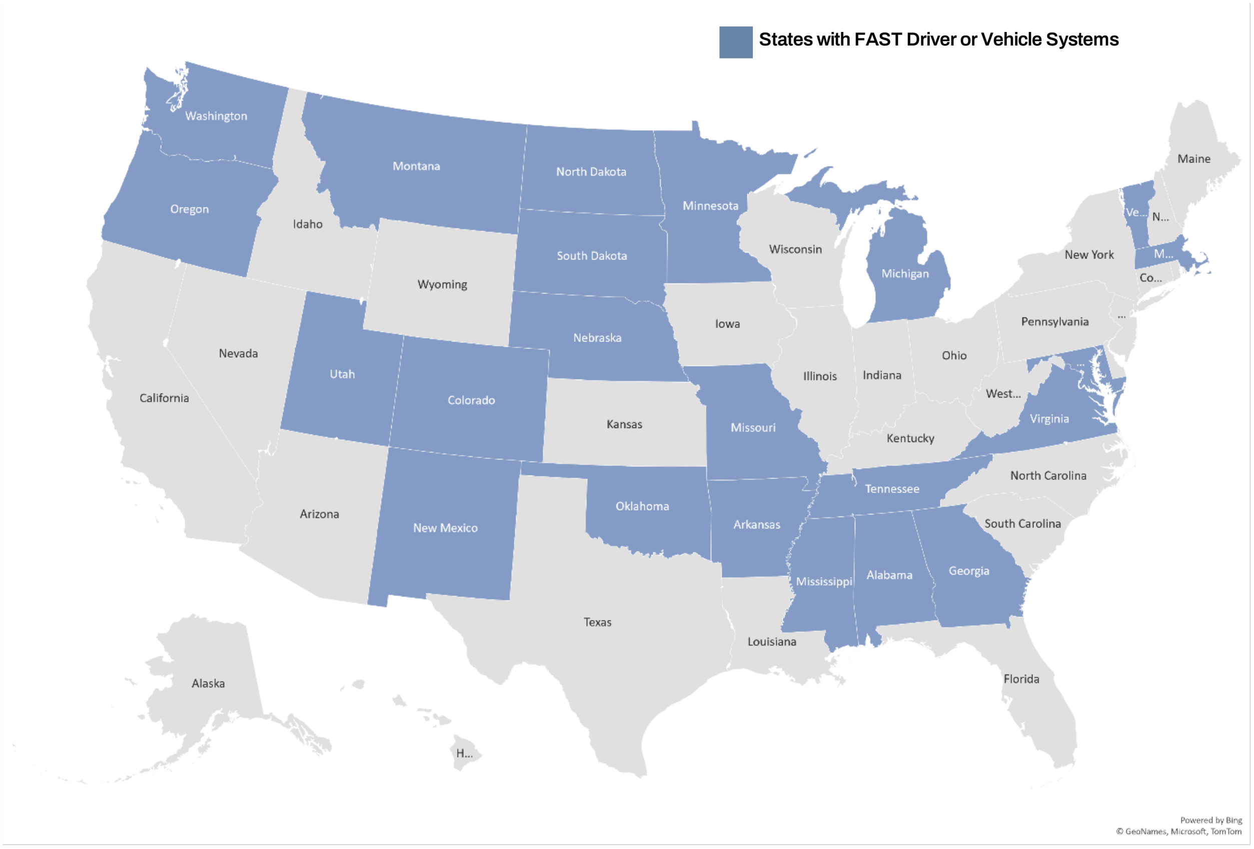
Access in real-time

OLIVR application allows for real-time data access, a feature used by many DMV partners, such as law enforcement and vehicle dealerships, which access greater than 141,000 records each day.

FAST Enterprises, contractor and developer of the OLIVR system, is implementing driver vehicle systems across the U.S.

In a strategic move to enhance its operational efficiency and service delivery, Oregon, through an open competitive procurement process, chose to hire FAST Enterprises (FAST), an established developer with a proven track record in the industry. This decision was influenced by the success of the FAST Driver and Vehicle System applications, which were first implemented by Arkansas in 2012 and have since been adopted by 22 states as of 2023. OLIVR is the implementation of the FastDS-VS® application configured for Oregon's use.

Figure 1: U.S. states with FAST Driver or Vehicle System applications in place as of 2023



Source: Auditor prepared based on information obtained from Fastenterprises.com

FAST's software solutions, including the OLIVR application, are already integral to various Oregon agency operations such as tax and revenue, employment, driver licensing and control, and vehicle titling and registration. These browser-based, platform-independent, and scalable applications are designed to reduce costs, enhance services, and improve internal operations, ensuring a high return on investment for the state.

Implementing the FAST software was a large and expensive undertaking for DMV. The FAST contract was worth $69.4 million and was part of the larger Service Transformation Project started by DMV; it included staff training and additional work in hopes of creating more efficient business processes. Per the ODOT 2023-2025 Legislatively Adopted Budget, the Service Transformation Project's $90 million, ten-year transformation of DMV computer systems, business processes and related technologies, which began during the 2015-17 biennium, was completed in the 21-23 biennium.

The implementation of OLIVR helped launch new services, expanding online services from three to 22, implementing improvements to DMV processes, and providing tools to help Oregonians use the new services through its DMV2U webpages. Offering more online services provides more convenience to customers, as well as improving efficiency for DMV operations to help keep costs down. As of January 2019, a variety of online services are available on DMV2U, where customers can:

- Schedule a DMV appointment;
- Replace a lost, mutilated, or stolen license or ID card;
- Upload a commercial driver medical examination certificate;
- Order a driving record;
- Pay a reinstatement fee; and
- Begin a driver license or identification card application for an initial issuance.

In May 2021, to provide better customer service, and help offset pressures on driver transaction volumes and wait times, DMV implemented online driver license and ID card renewals, allowing many Oregonians to avoid visiting an office in person. Future initiatives in various stages of development include installing self-service kiosks to improve customer service and the efficiency of offices and continued exploration of business process improvements and staffing strategies to increase the throughput of offices.

The purpose of this audit was to evaluate the effectiveness of key computer controls governing the OLIVR system and its data. Specifically, we evaluated controls governing data input, processing and output, programming changes, online service accessibility, and application security. These evaluations were intended to ensure that fees were being assessed appropriately, information was accessible to individuals who did not speak English well or who have disabilities, and people's personal information was protected.

Audit Results

We found OLIVR accurately assesses and collects fees for issuing Oregon drivers licenses and vehicle registrations and appropriately transfers information to the ODOT accounting system. However, more work needs to be done to improve accessibility via online services — specifically, to ensure that customers with disabilities, or who are not proficient in English, can access and use DMV's online portal for related driver and vehicle transactions.

Additionally, while we found the system was secure overall, additional improvements are needed to better secure the system and its data. Auditors found weaknesses relating to the department's processes for granting and reviewing employee system access, a lack of detailed application security plans, as well as a lack of appropriate periodic security risk assessments.

OLIVR accurately assesses and collects fees for driver license and identification issuance, vehicle registrations, and other vehicle transactions

DMV has designed and implemented controls to provide reasonable assurance that payment information remains complete, accurate, and valid during input, processing, and output for vehicle and driver related transactions in the OLIVR system.

Transactions entered and processed through computer systems should go through a variety of manual and automated procedures to ensure they are appropriate. In particular, procedures should ensure only complete, accurate, and valid information is entered into a system, data integrity is maintained during processing, and that system outputs meet expected results.

To achieve this, numerous controls have been implemented throughout the OLIVR system. These include:

- System validations that ensure input data match specified definitions for format and content, such as character set, length, numerical ranges, and acceptable values, and will not accept data that does not satisfy these definitions;
- Error messages and log entries that are created when input data is not accepted, or processing errors occur;
- Rejected input data or processing errors are held in suspense and identified on error reports until the errors are researched and resolved; and
- Logical access controls are implemented to ensure only authorized users have access to the system.

Oregon DMV issues approximately 200,000 new drivers' licenses and renews more than 350,000 licenses annually. The department also registers nearly 1.8 million vehicles, issues 850,000 titles, and issues roughly 400,000 vehicle plates — of which there are close to 50 different types of designs in addition to specialty and custom plates — all of which can dictate the fees assessed by OLIVR.

Figure 2: Title Fee Chart

Passenger vehicles and trucks (26,000 pounds GVWR or less)	Fee
Vehicle year is 1999 or older	$101
Vehicle year is 2000 or newer, has 0-19 combined MPG	$101
Vehicle year is 2000 or newer, has 20-39 combined MPG	$106
Vehicle year is 2000 or newer, has 40 combined MPG	$116
Electric vehicle	$192
Light trailer, travel trailers, motorcycles, mopeds, motor homes, buses, campers park model RVs, ATVs	$101
Heavy vehicle title	$90
Salvage title	$27
Late title transfer fee (31-60 days)	$25
Late title transfer fee (61 days or more)	$50

Source: DMV

Figure 3: Registration Fee Chart

Fee Type	When fee is due for passenger vehicles	Fee
Plate	Vehicle does not have Oregon plates	$26
Registration/ Renewal	Vehicle is 1999 or older	$126
	Vehicle year 2000 or newer, has combined rating of 0-19 MPG	$126
	Vehicle year 2000 or newer, has combined rating of 20-39 MPG	$136
	Vehicle year 2000 or newer, has combined rating of 40 MPG	$156
	Vehicle is all electric	$316
County	You reside and/or the vehicle stays in Multnomah County	$112
	You reside and/or the vehicle stays in Washington or Clackamas County	$60
Transfer Plates	Moving Oregon plates onto another vehicle (you will also owe the registration/county fees if you do not own the vehicle the plates were removed from)	$30

Source: DMV

We tested fees assessed for all driver and vehicle transactions, comprised of the types listed above as well as special interest plate fees, licensing fees, and testing fees, for fiscal year 2023. This equated to over 20 million rows of data. During testing, we found over 99.6% of transactions tested were complete, accurate, and valid, and confirmed that fees processed in OLIVR tied back to state statute, fee schedules, or other publicly available sources. Exceptions identified related to internal policies and accounting procedures and were determined to be unrelated to the design of the system, but rather division business decisions.

OLIVR accurately transfers information to ODOT's accounting system and other critical state and federal systems

OLIVR accurately and reliably transfers system transaction data into ODOT's main accounting system, the Transportation Environment Accounting and Management System, through an electronic interface daily. Additionally, OLIVR interfaces with over 200 other state and federal agencies, as well as partners, including the Department of Human Services, Oregon State Police, Department of Corrections, Department of Revenue, Oregon Secretary of State, and many more.

Controls surrounding interface processing should reasonably ensure data is transferred from the source system to the target system completely, accurately, and timely. Without these controls, the department would not be able to ensure fee revenue is accurately recorded, updates to Oregon's voter registry are completely transferred to the Secretary of State, or personal identification and vehicle ownership information is timely provided to state, local, and federal law enforcement agencies.

OLIVR uses multiple interface transfer methods, including direct system-to-system transfers using secure file transfer protocols, as well as a third-party fileshare where authorized parties can retrieve data files either manually or through automated processes. We Identified key interfaces based on various factors such as the type and quantity of data and found the division maintained appropriate documentation and key information as recommended by industry best practices.

Auditors reviewed reconciliations performed between the OLIVR and the Transportation Environment Accounting and Management System, observed logs showing successful transfers between systems, and reviewed processes to identify and resolve interface errors. We found the department maintains extensive logs and has appropriate processes in place that allow for the observation, identification, and remediation of any issues encountered during a data handshake; that is, when data is pushed and pulled via the interface.

Oregon DMV's public web portal lacks appropriate accessibility features such as multi-language support and support for the visually impaired

More work needs to be done to ensure DMV services meet the needs of all Oregonians, including those with limited or no English proficiency as well as those with disabilities, such as the visually impaired.

As part of its strategic plan, which includes the DMV, ODOT has included specific equity goals. Specifically, DMV's equity goal states: "DMV will be able to identify and respond to the needs of all Oregonians by equitably connecting access opportunities to DMV services, account for location, mobility, language, race, gender, and more." Based on this, we performed procedures to determine whether the OLIVR application provides effective controls to ensure web content is accessible to persons with disabilities and has appropriate language translations for non-English speaking users that is both intuitive and consistent for all DMV customers in Oregon.

Some measures have been taken to help ensure Oregon DMV web content is accessible to persons with disabilities, and has appropriate language alternatives for customers who do not speak English or have limited English proficiency. Yet we determined more work needs to be done to ensure these customers have access to DMV services through the DMV2U web portal.

Specifically, we found the main DMV site has built-in language translation services, but upon navigating to the DMV2U service portal, these language translation services are no longer supported. Instead, Oregon relies on Google Translate within the web browser to translate to other languages. However, we found this was not intuitive for users, was inconsistent across pages, was unsupported on mobile devices, and, depending on the browser, would often error out or otherwise was unable to translate the site. As approximately 15% of people living in Oregon are non-English speakers, this significantly impacts their ability to utilize online services at Oregon DMV.

Additionally, we noted Oregon DMV does not utilize all best practices for website accessibility for people with disabilities. Specifically, DMV2U does not include alt-text for graphic or picture elements, or the use of shading on required fields for visually impaired customers.

As part of the project implementation, FAST contracted with Lebsontech, LLC to conduct a usability study to identify potential user-interface issues and areas of potential improvement for the e-services provided to the public. In reviewing the study, we noted that the users were largely college educated English speaking users. None of the key concerns listed in the study noted the language translation problems, or the accessibility issues. As such, we determined accessibility features and language support were likely overlooked.

Application security support processes should be improved to better protect the system and its data

Department management has implemented important protection measures for system security such as multifactor authentication, system logging, and role-based access, but additional process improvements are needed to better secure the system and its data. Weaknesses included immature processes for granting and reviewing employee system access, a lack of detailed application security plans, as well as a lack of appropriate periodic security risk assessments.

User account management needs improvement

The OLIVR application uses role-based access and has appropriate roles and separation of duties. However, user account management processes governing access to OLIVR are not sufficient to ensure DMV employees only have access to system functionality needed to perform their duties.

Access to computer applications should be restricted according to each user's individual need to view, add, or alter information. In order to maintain this principle of "least privilege," organizations should have formal processes for timely granting, suspending, and closing user accounts. Management should also periodically review and confirm users' access rights to ensure they remain appropriate.

We reviewed processes the department staff use to grant and maintain users' access to the system and identified several procedures that need improvement. Specifically, we found:

- DMV lacks comprehensive policies, processes, and procedures for provisioning, monitoring, reviewing, and removing employee access to the OLIVR system;
- Periodic review of OLIVR user access has not been performed;
- Terminated employees are not always timely removed from the system; and
- Inactive or users who have never logged into the system are not timely removed from the system.

We tested all 1,056 users with access to the OLIVR system and found 44 stale accounts, two active accounts for terminated employees, 11 active accounts that were never logged into, and 45 accounts that had not been logged into in over a year. These weaknesses increase the likelihood that users will have more access to the system than they need to perform their duties, and that the system and its data could be compromised.

OLIVR password parameters were insufficient and did not meet statewide standards

During fieldwork testing, we determined OLIVR password parameters were insufficient and not in compliance with Statewide Information Technology Control Standards.[1] Access controls necessitate user authentication using secret passwords or other identifiers. These controls restrict authenticated users' access to data, files and resources, as well as the actions they can perform.

Oregon Statewide Information Technology Control Standards were updated in January 2024 to require a system password be at least 15 characters in length with additional complexity requirement for more sensitive data. We noted as of July 2024 OLIVR did not meet one or more of these requirements.

Without robust access controls, unauthorized individuals can clandestinely access sensitive data, copy it, and potentially make undetected alterations or deletions for malicious intent or personal gain.

Application security management program for OLIVR is missing important elements

More work is needed to ensure security management processes are appropriate and are properly securing the application and its environment.

Effective application security management provides a foundation for department management to obtain reasonable assurance the application is secure. It provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's application-related controls. The necessary steps include:

- Establishing an application security plan;
- Periodically assessing and validating application security risks;
- Documenting and implementing application security policies and procedures;
- Monitoring the effectiveness of the security program; and
- Remediating information security weaknesses.

While some elements of the application security management program are in place, more work is needed to properly secure the application and its environment. This includes:

- Documenting a formal application security plan;
- Performing appropriate and timely application risk assessments; and
- Documenting application security policies and procedures, including separation of duties and proper handling of master data.

Additionally, Oregon Statewide Information Technology Control Standards requires that in circumstances where security standards cannot be implemented, agencies must document deviations and indicate the compensating controls that have been applied to adequately protect systems or information. Deviations must be signed by the agency's director and filed with Oregon's Enterprise Information Services (EIS)

[1] Oregon Statewide Information Technology Control Standards

department per statewide policy.[2] We found the department had not filed agency-identified security deviations with EIS at the time of our audit.

Without effective security management over the application, there is an increased risk that management, information technology staff, and application owners will not properly assess risk and will, consequently, implement inappropriate or inadequate information security controls over the application.

Change management processes supporting OLIVR are appropriately implemented and effective

OLIVR computer code modifications are appropriately controlled to ensure the integrity of the system data is maintained.

Changes to computer applications should be managed to ensure only tested and approved modifications are placed into production. The system vendor, FAST, controls and maintains the OLIVR source code for core functions. DMV programming staff have access to and can make changes to code specific to Oregon and the changes it needs specific to state needs.

We reviewed the process for implementing OLIVR updates to ensure proper authorization exists for system patching, system updates are tested prior to implementing in production, and appropriate change management review processes are followed.

During fiscal year 2023 there were 426 significant change request tickets that were implemented for the OLIVR system. Using a statistically valid sample plan, we tested approximately 14% of these change request tickets and found all of them followed the appropriate process. As such, we determined changes to OLIVR computer code are appropriately controlled and implemented.

[2] Department of Administrative Services Statewide Policy 107-004-052

Recommendations

To ensure the OLIVR application's public web portal, DMV2U, is accessible to all users, we recommend DMV:

1. Integrate language translations services into the DMV2U public portal that is compatible with most commonly used browsers and optimized for mobile devices.

2. Adopt alt-text and other accessibility features into DMV2U.

3. Include a more diverse user group for future usability studies that better reflects customer demographics, including non-English speakers, and those with disabilities, such as the visually impaired, to ensure online services are more accessible to all customers.

To better secure the OLIVR application and its environment, we recommend DMV:

4. Create, document, and implement policies, processes, and procedures for user account management to ensure a routine, repeatable process is performed. This should include but is not limited to:

    a. Provisioning access for new users;

    b. Periodic review of access to ensure it remains appropriate; and

    c. Removing access for inactive or terminated users.

5. Ensure application password parameters meet Statewide Information Technology Control Standards.

6. Develop an Application Security Plan specific to OLIVR.

7. Perform periodic risk assessments of the OLIVR application to ensure security risks are timely identified and remediated.

8. Update related security policies and procedures for the OLIVR application, including, but not limited to, documenting separation of duties, identification of sensitive transactions, and master data handling.

9. When Statewide Information Technology Control Standards cannot be implemented, ensure appropriate exception documentation is signed by the agency head and filed with EIS per statewide policy 107-004-052.

Objective, Scope, and Methodology

OBJECTIVE

- Determine whether information system controls at DMV governing the OLIVR system provide reasonable assurance that transaction data remains complete, accurate and valid during input, processing and output.
- Determine whether the OLIVR application provides effective controls to ensure web content is accessible to persons with disabilities and appropriate language alternatives customers who do not speak English or have limited English proficiency, that is intuitive and consistent for all DMV customers.
- Determine whether information system controls at DMV governing the OLIVR system provide reasonable assurance that system information is protected against unauthorized use, disclosure, modification, damage, or loss.
- Determine whether information system controls at DMV governing the OLIVR system provide reasonable assurance that changes to computer code and configurations are managed to ensure integrity of the system and that only approved program modifications are implemented.

SCOPE

Our scope for the audit, relating to IT application controls, focused on financial transactions processed within the application. Specifically, we looked at all vehicle and driver-related transactions where a fee was assessed for an individual customer during fiscal year 2023.

While our focus was on the OLIVR application, we reviewed website and user portal accessibility as well as general IT controls at the enterprise, agency, and division level. General IT controls centered around security, which are typically handled at the agency or enterprise-level rather than the division level. As such, we considered the policies, practices, and procedures at the agency and enterprise-level as they pertained to the DMV and then to OLIVR specifically where applicable.

METHODOLOGY

To understand the application and its environment, IT auditors conducted research, interviewed ODOT and DMV employees, and observed how work was conducted. This process involves interviewing agency personnel; gathering agency documentation, including internal policies, processes and procedures to review; and inspecting the agency's internal controls system used to ensure the entity reaches its intended objectives.

Auditors tested over 20 million transaction records to ensure vehicle and driver transaction fees were appropriate for the service provided, as well as determining whether county fees were appropriately applied. Auditors did not review whether vehicles were assigned the appropriate MPG rating, as this action is performed by a third-party entity. Additionally, we reviewed all access to the system by DMV employees and contractors, reviewed change tickets to ensure all changes were appropriate, and reviewed application security policies and procedures. Auditors also ran accessibility tests on DMV's public portal DMV2U.

The criteria for our audit included the Government Accountability Office's publication "Federal Information System Controls Audit Manual (FISCAM)"; the ISACA publication "COBIT 2019 Framework – Governance and Management Controls”; industry best practices, including a review of what other states have performed; and, where applicable, state laws, regulations, and statutes.

Our inspection and observation included review of:

- Other states’ FastDS-VS® best practices;
- Oregon ODOT and DMV statutes, policies and procedures;
- Presentations to legislators;
- Review of segregation of duties, roles, and groups;
- Security training and training records;
- Agency security breach reporting;
- Oregon Consumer Privacy Act;
- Breach reporting standards for the Oregon Consumer Identity Theft Protection Act; and
- Funding and budgeting documentation.

INTERNAL CONTROL REVIEW

We determined the following internal controls were relevant to our audit objectives and considered:[3]

- Control Environment
    - Whether management oversees the entity’s internal control system.
- Risk Assessment
    - Whether management defines objectives clearly to enable the identification of risks and define risk tolerances.
    - Whether management identifies, analyzes and responds to risks related to achieving the defined objectives.
    - Whether management considers the potential for fraud when identifying, analyzing and responding to risks.
    - Whether management identifies, analyzes and responds to significant changes that could impact the internal control system.
- Control activities
    - Whether management has designed control activities to achieve objectives and respond to risks.
    - Whether management designed the entity’s information system and related control activities to achieve objectives and respond to risks.
    - Whether management has implemented control activities through policies.
- Information and communication
    - Whether management uses quality information to achieve the entity’s objectives.
- Monitoring activities
    - Whether management has established and operates monitoring activities to monitor the internal control system and evaluate the results.
    - Whether management remediates identified internal control deficiencies on a timely basis.

[3] Auditors relied on standards for internal controls from the U.S. Government Accountability Office, report GAO-14-704G

Deficiencies with these internal controls are documented in the results section of this report.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We sincerely appreciate the courtesies and cooperation extended by employees of ODOT and DMV during this audit.

Audit team

Erika Ungern, CISA, CISSP, Audit Manager
Matthew Owens, MBA, CISA, Principal Auditor
Julie Moffenbier, M.Acc, Senior Auditor
Sheila Faulkner, Staff Auditor

ABOUT THE SECRETARY OF STATE AUDITS DIVISION

The Oregon Constitution provides that the Secretary of State shall be, by virtue of the office, Auditor of Public Accounts. The Audits Division performs this duty. The division reports to the Secretary of State and is independent of other agencies within the Executive, Legislative, and Judicial branches of Oregon government. The division has constitutional authority to audit all state officers, agencies, boards and commissions as well as administer municipal audit law.

Oregon

Tina Kotek, Governor

Department of Transportation
Driver and Motor Vehicle Services - DMV
1905 Lana Ave NE
Salem, OR 97314-5000
www.OregonDMV.com

September 12, 2024

Kip Memmott, Director
Secretary of State, Audits Division
255 Capitol St. NE, Suite 180
Salem, OR 97310

Dear Mr. Memmott,

This letter provides a written response to the Audits Division's final draft audit report titled "Licensing and Registration System Accurately Assesses and Collects Fees, but Security Processes Need Improvement."

The Oregon Department of Transportation (ODOT), Driver and Motor Vehicle Services Division (DMV), appreciates the Secretary of State, Audit Division's, work to understand and evaluate our Oregon License Issuance and Vehicle Registration (OLIVR) system. We are pleased that you found the OLIVR system accurately assesses and collects fees, and that it accurately and reliably transfers system transaction data into ODOT's main accounting system. We are also pleased that you found OLIVR computer code modifications are appropriately controlled and that the integrity of the system data is maintained.

We agree more can be done to ensure DMV's online (web) services are accessible to all. We also agree that greater monitoring of staff access, including provisioning and deprovisioning in OLIVR, is needed. And we agree that the agency must meet Statewide Technology Standards, perform periodic risk assessments, and keep security policies and procedures up to date.

Below is our detailed response to each recommendation in the audit.

<table>
<tr><td colspan="3"><b>RECOMMENDATION 1</b>
To ensure the OLIVR application's public web portal, DMV2U, is accessible to all users, we recommend DMV integrate language translations services into the DMV2U public portal that is compatible with most commonly used browsers and optimized for mobile devices.</td></tr>
<tr><th>Agree or Disagree with Recommendation</th><th>Target date to complete implementation activities</th><th>Name and phone number of specific point of contact for implementation</th></tr>
<tr><td>Agree</td><td>March 31, 2026</td><td>Ben Kahn, DMV Innovation and Planning Manager
503-945-5353</td></tr>
</table>

Narrative for Recommendation 1

DMV agrees with Recommendation 1 and is launching a project to improve accessibility for all users, including integrating Spanish language translation services in the DMV2U public portal. Given the scope of the project and the need for DMV to seek input from third party translation services, this effort has a completion target in 2026. This aligns with DMV's Strategic Priority of Clear Customer Communication.

RECOMMENDATION 2

To ensure the OLIVR application's public web portal, DMV2U, is accessible to all users, we recommend DMV adopt alt-text and other accessibility features into DMV2U.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	September 30, 2025	Ben Kahn, DMV Innovation and Planning Manager 503-945-5353

Narrative for Recommendation 2

DMV agrees with Recommendation 2 and will be adopting alt-text as well as other accessibility features into DMV2U. While full implementation will be accomplished in late 2025, we will pursue the implementation of incremental changes well before that date. This effort aligns with DMV's Strategic Priority of Clear Customer Communication.

RECOMMENDATION 3

To ensure the OLIVR application's public web portal, DMV2U, is accessible to all users, we recommend DMV include a more diverse user group for future usability studies that better reflects customer demographics, including non-English speakers, and those with disabilities, such as the visually impaired, to ensure online services are more accessible to all customers.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	Implemented May 25, 2023	Lisa Martinez, DMV Change and Engagement Manager, 503-779-5098

Narrative for Recommendation 3

DMV agrees with Recommendation 3 and has already implemented improved User Experience (UX) Testing in May 2023 with a more diverse group of participants, including non-English speakers, and those with disabilities, including the visually and hearing impaired. This aligns with DMV's Strategic Priority of Clear Customer Communication.

RECOMMENDATION 4

To better secure the OLIVR application and its environment, we recommend DMV Create, document, and implement policies, processes, and procedures for user account management to ensure a routine, repeatable process is performed. This should include but is not limited to:

1. Provisioning access for new users;
2. Periodic review of access to ensure it remains appropriate; and
3. Removing access for inactive or terminated users.

Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	July 31, 2025	Michael Hemsley, DMV Business Systems Support Manager, 503-586-8585

Narrative for Recommendation 4

DMV agrees with Recommendation 4 and has formed a workgroup to implement additional documentation and process monitoring for provisioning access for new users, doing periodic reviews of access to ensure it remains appropriate, and removing access for inactive or terminated users. DMV will take immediate action to remove inactive or terminated users while the overall process improvements are being worked out.

RECOMMENDATION 5

To better secure the OLIVR application and its environment, we recommend DMV ensure application password parameters meet Statewide Information Technology Control Standards.

Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	Implemented August 1, 2024	Karina Stewart, ODOT Information Security Officer, 503-986-4397

Narrative for Recommendation 5

DMV agrees with Recommendation 5 and implemented password standards that adhere to the Statewide Information Technology Control Standards on August 1, 2024.

RECOMMENDATION 6

To better secure the OLIVR application and its environment, we recommend DMV develop an Application Security Plan specific to OLIVR.

Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**

Agree	April 1, 2025	Karina Stewart, ODOT Information Security Officer, 503-986-4397

Narrative for Recommendation 6
DMV agrees with Recommendation 6 and will work with ODOT IT Security to complete a System Security Plan specific to OLIVR. Any security issues identified while carrying out the security plan will be addressed immediately.

RECOMMENDATION 7
To better secure the OLIVR application and its environment, we recommend DMV perform periodic risk assessments of the OLIVR application to ensure security risks are timely identified and remediated.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	July 1, 2025	Karina Stewart, ODOT Information Security Officer, 503-986-4397

Narrative for Recommendation 7
DMV agrees with Recommendation 7 and will work with ODOT IT Security as they do periodic risk assessments of the OLIVR application. Any security issues identified while doing the risk assessments will be addressed immediately.

RECOMMENDATION 8
To better secure the OLIVR application and its environment, we recommend DMV update related security policies and procedures for the OLIVR application, including, but not limited to, documenting separation of duties, identification of sensitive transactions, and master data handling.

Agree or Disagree with Recommendation	Target date to complete implementation activities	Name and phone number of specific point of contact for implementation
Agree	September 1, 2025	Karina Stewart, ODOT Information Security Officer, 503-986-4397

Narrative for Recommendation 8
DMV agrees with Recommendation 8 and will work with ODOT IT Security to update related security policies and procedures for the OLIVR application. These will include documenting separation of duties, identifying sensitive transactions, and master data

handling. To ensure Statewide Technology Standards are met, ODOT IT Security will need to consult with other entities like Enterprise Information Services. Immediate action will be taken on any circumstances where these updated policies and/or procedures are not adhered to.

RECOMMENDATION 9
To better secure the OLIVR application and its environment, we recommend DMV, when Statewide Information Technology Control Standards cannot be implemented, ensure appropriate exception documentation is signed by the agency head and filed with EIS per statewide policy 107-004-052.

Agree or Disagree with Recommendation	**Target date to complete implementation activities**	**Name and phone number of specific point of contact for implementation**
Agree	November 30, 2024	Karina Stewart, ODOT Information Security Officer, 503-986-4397

Narrative for Recommendation 9
DMV agrees with Recommendation 9 and will work with ODOT IT Security to ensure Statewide Information Technology Control Standards are met. Appropriate exception documentation will be submitted when Standards are not met.

Please contact Ben Kahn, ODOT DMV Innovation and Planning Manager, at 503-945-5353 with any questions.

Sincerely,

Amy Joyce

Amy Joyce
DMV Administrator

cc: Kris Strickler, ODOT Director
Travis Brouwer, ODOT Assistant Director
Marlene Hartinger, ODOT Chief Auditor

Oregon Secretary *of* State
Audits Division

Secretary of State **LaVonne Griffin-Valade**
Audits Director **Kip R. Memmott**

This report is intended to promote the best possible management of public resources.

Copies may be obtained from:

Oregon Audits Division
255 Capitol St NE, Suite 180
Salem OR 97310
(503) 986-2255

audits.sos@oregon.gov
sos.oregon.gov/audits