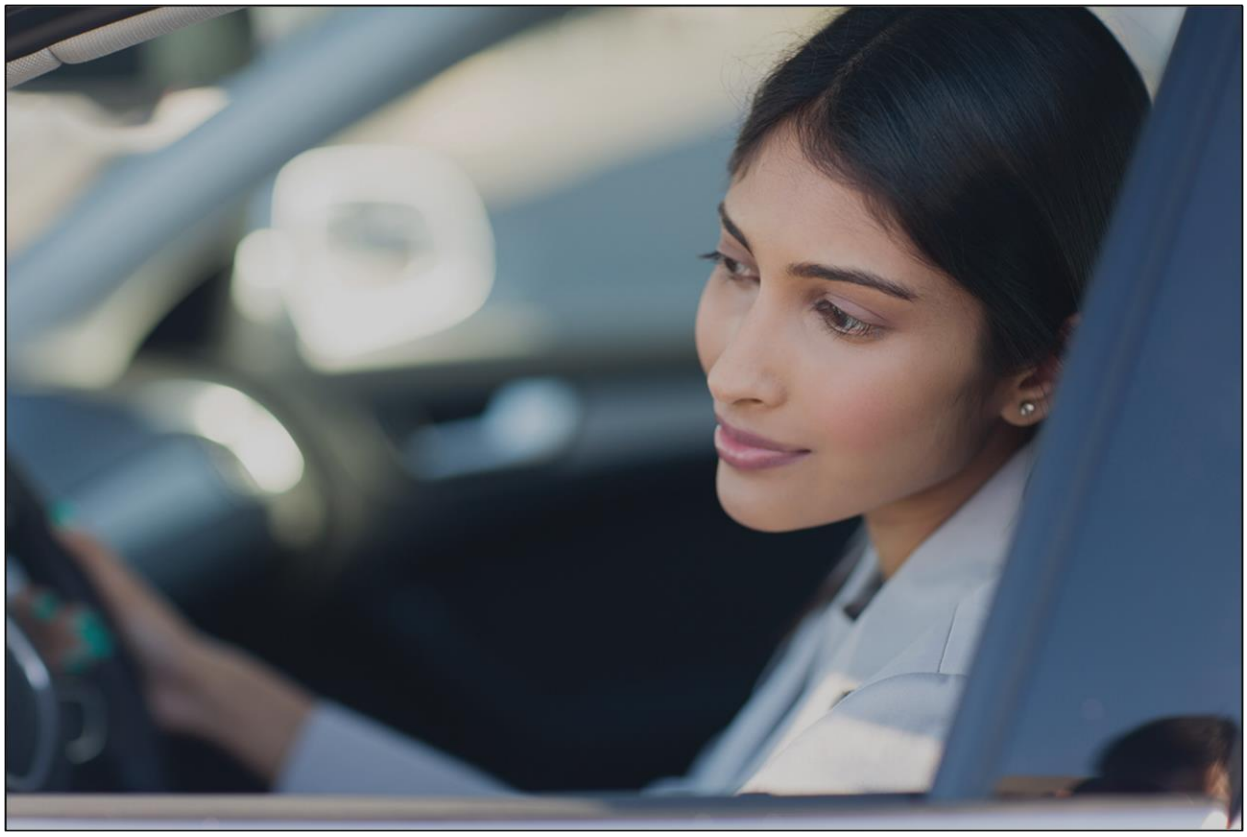
WASHINGTON STATE DEPARTMENT OF LICENSING

DOL Customer Data Protections Quarterly Report June 1, 2026



Washington State Department of Licensing

Quarterly Report

June 2026

ADA Accessibility

If you need accommodation to access this material, our services, or our facilities, call 360-902-3900. If you're deaf or hard of hearing, call 711 for relay services. You can also find more information on our website at dol.wa.gov/accessibility. If you believe your rights to receive an accommodation under the Americans with Disabilities Act (ADA) have been denied, contact our ADA Compliance Manager at ada@dol.wa.gov or at the phone numbers listed above.

Contact Information

Molly Voris
Legislative and Policy Director
Department of Licensing
Molly.Voris@dol.wa.gov

https://dol.wa.gov/about/reports-and-data/reports-legislature

Related Information

- DOL open data published on data.wa.gov:

  https://data.wa.gov/browse?q=department%20of%20licensing

- DOL self-service data lookup tools: Driver and Plate Search (DAPS) and Driver Information and Adjudication System (DIAS)

  a. General description: https://dol.wa.gov/driver-and-plate-search-daps-and-driver-information-and-adjudication-system-dias

  b. Application for service: https://dol.wa.gov/driver-and-plate-search-daps-and-driver-information-and-adjudication-system-dias

  c. Data Sharing agreement: https://dol.wa.gov/media/pdf/2423/interagency-data-sharing-agreement-drives-accesspdf/download?inline

Table of Contents

Executive Summary 4

Background 5

Part A. The Keep Washington Working and Executive Order 25-09 7

- Implementing the Keep Washington Working Act 7
- Governing DOL data systems: DAPS and DIAS 8
- Implementing Executive Order 25-09 16

Part B. DAPS and DIAS Statistical Reporting 18

Part C. ACCESS and Nlets Statistical Reporting 20

Part D. Appendix A and Glossary of Terms 22

Executive Summary

Washington state is a national leader in personal data protection. As the federal government has rapidly changed its tactics and the way it uses state data, Governor Ferguson has continually considered and reassessed state agencies' data practices and taken quick action when necessary. Additionally, Department of Licensing (DOL) has been taking actions to protect consumer data for the last several years.

DOL has cancelled DAPS (Driver and Plate Search) access for two federal agencies—Immigration and Customs Enforcement (ICE) and Homeland Security Investigations (HSI)—and has suspended access for several other federal agencies that have not met the state's requirements for authorized access to this data. Second, DOL and Washington State Patrol (WSP) have blocked all searches of DOL data by Originating Agency Identifiers (ORIs) associated with ICE (including HSI and Enforcement and Removal Operations (ERO)). There are only a handful of states that have taken this step, and Washington is one of them.

ORIs are a nine-character code assigned by the FBI to identify a specific criminal justice or public safety agency that sends or receives messages through Nlets. Nlets is a law enforcement data exchange, also referred to as a "switch," that is accessible to all fifty states and their localities, certain Canadian jurisdictions, Interpol, and federal agencies. Nlets allows law enforcement at all levels to query databases, such as a state's driver and vehicle records, criminal records, and corrections records. Shutting off the federal government's access to DOL data across the board is not an option because there are many legitimate public safety reasons why Washington needs to share data with some federal law enforcement agencies—such as preventing violent crime, child abductions, and human trafficking.

Customs and Border Protection (CBP) is a federal agency that has important responsibilities related to border security, customs and imports, and counterterrorism. The state is currently assessing CBP's use of Nlets to search state DOL data and what steps the state might take to protect Washingtonians' data without compromising law enforcement functions that keep Washingtonians safe. The state is taking the following steps to protect Washingtonians' privacy: (1) removed CBP's ability to see photos of Washingtonians in Nlets (which no other state has proactively done) and (2) currently reviewing a list of CBP ORIs that are suspected to be directly associated with civil immigration enforcement.

The following report gives an overview of DOL's actions to protect personal individual information from misuse. The report also presents statistical data showing how federal,

state, and local agencies use the Driver and Plate Search (DAPS) and Driver Information and Adjudication System (DIAS).

With the resources provided by the Legislature in fiscal year 2027, and in collaboration with the Washington State Patrol (WSP), DOL is collecting data on the independent nationwide system known as the International Justice and Public Safety Network, Nlets. DOL will present equivalent statistical information for that system in future reports, starting in September 2026.

Background

DOL developed this report to comply with Proviso 31 of the state's 2026 transportation budget bill, ESSB 6005, Chapter 257, Laws of 2026, which provides:

> $200,000 of the highway safety account—state appropriation is provided solely to implement a quarterly reporting of statistical information and a status report on the actions taken to protect personal individual data from misuse, particularly for immigrant communities. Beginning June 1, 2026, and quarterly thereafter, the department must include a breakout, by federal, state, and local agency, on the number of queries on Washington driver's license or identicard holders in the following systems: Driver and plate search (DAPS); and the driver information and adjudication system (DIAS). Beginning June 1, 2026, the department must collect statistical information from the Washington state patrol on queries received from Nlets system and ACCESS terminals, of Washington driver's license or identicard records. This data must identify the number of incoming queries, broken out by federal and state agencies that access Washington systems via Nlets and ACCESS terminals. The number of queries from state and local agencies outside of Washington may be grouped by state. The data on the number of incoming queries must include the message keys used and a general description of data provided by each message key used. The quarterly report must also include information on the current federal, state, and local agencies that are allowed and denied access. The first quarterly report must include detailed information on the actions the department has taken in the prior months to ensure compliance with chapter 440, Laws of 2019 (Keep Washington Working Act), and the Governor's executive order 25-09.[1]

This report, the first quarterly report, is divided into the following sections:

Part A. The Keep Washington Working Act and Executive Order 25-09

> The first quarterly report must include detailed information on DOL's actions to ensure compliance with chapter 440, Laws of 2019 (Keep Washington Working Act),

[1] https://lawfilesext.leg.wa.gov/biennium/2025-26/Pdf/Bills/Session%20Laws/Senate/6005-S.SL.pdf#page=40

and the Governor Ferguson's Executive Order 25-09: Reaffirming Washington's Commitment to Protecting the Rights and Interests of Immigrant Communities.

Part B. DAPS/DIAS Statistical Reporting

Beginning June 1, 2026, DOL must submit quarterly reports that include the number of queries on Washington driver license or identicard holders in the driver and plate search (DAPS) and driver information and adjudication systems (DIAS). The reports must show information about queries from federal, state, and local agencies.

Part C. ACCESS and Nlets Statistical Reporting

DOL just recently started collecting statistical information about Nlets through DRIVES, DOL's system of record for identification, drivers, and vehicles. Using fiscal year 2027 funds provided by the budget, DOL will study the Nlets data and include an analysis in its second quarterly report, planned for September 2026. If feasible and appropriate, DOL also intends to publish anonymized raw data for independent analysis.

Part D. Appendix A and Glossary of Terms

Part A. Keep Washington Working and Executive Order 25-09

Immigration enforcement has become a key policy issue in recent years, and DOL's role as the steward of essential identity information for Washington residents has brought additional attention to the agency. As directed by Proviso 31, the sections that follow explain the agency's approach, goals, and initiatives tuned to comply with Washington's laws, policy objectives, and values.

Implementing the Keep Washington Working Act

Together with the Governor's Office, legislators, and immigrant advocates, DOL reengineered its process for responding to driver license record requests from local, state, and federal law enforcement agencies in 2018 in several ways. In doing so, DOL strove to prioritize data protections without compromising legitimate public safety interests that are served by sharing some forms of data.

In 2019, Governor Inslee signed the bipartisan Keep Washington Working Act (KWW) into law. KWW built upon several key privacy laws and orders already in force, including the federal Driver's Protection and Privacy Act of 1994 (DPPA); Executive Order 16-01 (Modernizing State Agency Privacy Protection); and Executive Order 17-01 (Reaffirming Washington's Commitment to Tolerance, Diversity, and Inclusiveness). DOL's compliance with KWW built upon the measures already in place from the previous year.

Between 2018 and 2024, DOL:

- Discontinued access to DAPS for ICE-ERO (Enforcement and Removal Operations) and required all other users to certify the tool will not be used for immigration enforcement.
- Removed multiple data fields, including Social Security Numbers, from DAPS, Nlets, and ACCESS.
- Established a multi-tiered review process for federal agency records requests.
- Incorporated language upholding KWW into all data sharing agreements.
- Began auditing private data partners for compliance with Executive Order 17-01 and Keep Washington Working.
- Built a robust data-privacy framework and created a data-management office.

- Created policies, training, and other accountability measures to ensure DOL staff strictly adhere to all data sharing prohibitions.

Since 2025, under Governor Ferguson's leadership, DOL and WSP have taken additional measures to protect customer data. These include:

- Ending ICE-HSI (Homeland Security Investigations) access to DAPS.
- Suspending DAPS access for DHS and its subagency CBP (Customs and Border Protection).
- Ending ICE-ERO's and ICE-HSI's access to driver and vehicle data through Nlets.
- Ending CBP's access to driver photographs through Nlets.
- Investigating CBP usage of the Nlets system for civil immigration purposes and suspending access where there was evidence of using DOL data for civil immigration enforcement.

Governing DOL data systems: DAPS and DIAS

There are several ways authorized law enforcement organizations and courts can look up information in DOL's data systems, using a self-service model in addition to written requests answered by staff or using the State Patrol's ACCESS system for law enforcement.

DAPS. The Driver and Plate Search (DAPS) system was designed as a web-based search tool for use by law enforcement and other government entities. It allows authorized users to search for driver, vehicle, and vessel records. DAPS allows for search term expanders to return broad search results. For example, a user searching for "Kell* Sm*th" would see results for Kelly, Kellie, Kelley, Kellan and Smith or Smyth). Likewise, a user searching for plate number ABC123* would see results for ABC1234, ABC1235, etc.

DOL shares the following data fields through DAPS:

- Full name
- Date of birth
- Driver license number
- Address
- Physical identifying features (height, weight, eye color)
- Driving status – restrictions and endorsements

- Vehicles/license plates/VIN numbers

Authorized organizations must designate an administrator, who is responsible for compliance with the service's data sharing agreement and who enables and disables staff accounts within their organization.

Authorized users can access the DAPS system through License Express, DOL's secure portal for eservices. License Express is authenticated by Secure Access Washington, the state's secure login gateway.

Washington state law enforcement, including municipal and county organizations, and certain federal agencies, have access to DAPS. Department of Homeland Security offices, including Immigration and Customs Enforcement and Customs and Border Protection, do not have access to DAPS.

DIAS. The Driver Information and Adjudication System (DIAS) allows courts to electronically access and update DOL driver records. DIAS users can:

- Add and adjudicate unresolved traffic citations.
- Submit and correct court convictions, deferred prosecution, and pre-trial ignition interlock requirements.
- Submit a judgment for motor vehicle loss.
- Search and access driver records.
- Request certified copies of driver records.
- Request certified copies of driver photos.
- Request address history.
- Request registration holds to enforce parking fines.

Managing DAPS and DIAS to comply with the Keep Washington Working Act

DAPS and DIAS are powerful search systems that could harm Washington residents if used improperly. All organizations using these systems are required to participate in a compliance program, which DOL oversees. The agency can suspend or terminate access for those who do not comply.

Compliance requirements for organizations using the services

To get a DAPS or DIAS account, an organization must:

- Apply to DOL.
- Provide a detailed explanation of why they need access to these programs and whether they will disclose what they learn to other parties.
- Name an authorized administrator.
- Confirm they understand their organization must not use DOL data for investigating, locating, or apprehending individuals for immigration-related violations.

These applications are carefully reviewed by DOL staff, and many applicants are asked about any possible links to civil immigration enforcement. Some applications are denied due to concerns about incomplete information, conflicts of interest, or the organization's purpose and activities.

Key provisions of the DAPS/DIAS data sharing agreement

Data may only be used for lawful actions related to the licensee's functions as a government agency, the purposes in the licensee's application, and as approved by DOL. All other use of data is strictly prohibited. DOL has the right to re-determine its approval for permitted uses and may cancel or restrict access if uses do not comply with state law or DOL policy. Investigating, locating, or apprehending individuals for civil immigration-related violations is strictly prohibited.

Suspension and termination of DAPS/DIAS accounts for noncompliance

DAPS and DIAS user organizations must conduct an annual self-assessment, signed by the account administrator, which confirms that the organizations are complying with all data sharing agreement requirements, including the Keep Washington Working Act. See Figure 5 below for an example. As a result of DOL's active and developing management of the DAPS and DIAS systems, several accounts and organizations have had their access suspended or terminated in recent years. Tables 3 through 5 reflect suspensions and terminations implemented since 2024.

In August of 2025, the Department of Licensing learned about misuse of DAPS data by Homeland Security. DOL took immediate action and terminated the offending account's access, as well as that of related accounts that were identified afterwards.

Table 1. Accounts terminated for improper use

Date terminated	Account number	Agency name	Service
8/27/2025	DPS-095433	U.S. ICE, HOMELAND SECURITY, INVESTIGATIONS	DAPS
9/2/2025	DPS-959593	DHS-ICE-HSI	DAPS
11/19/2025[2]	DPS-832300	U.S. DEPT OF HOMELAND SECURITY	DAPS

Each year, DOL performs compliance activities on its eservice accounts. This includes obtaining an annual attestation from the account administrator that all searches were performed in compliance with the data sharing agreement terms. Failure to submit the required attestation can result in the suspension of access.

The accounts in Table 4 were suspended for noncompliance with this requirement in September 2025. Per the terms of the DAPS interagency data sharing agreement, accounts suspended longer than ninety (90) days are terminated automatically. Therefore, the following accounts are no longer active.

[2] This account failed to have an identified administrator and was administratively terminated.

Table 4. Administratively suspended accounts as of March 31, 2026

Suspension date	Account number	Agency name	Service
2/24/2026	DIS-591736	U.S. ENVIRONMENTAL PROTECTION AGENCY – CRIMINAL INVESTIGATION DIVISION	DIAS
9/4/2025	DPS-903029	AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS	DAPS
9/4/2025	DPS-205995	DEA SPOKANE	DAPS
9/4/2025	DPS-881775	MADIGAN ARMY MEDICAL CENTER	DAPS
9/4/2025	DPS-935019	NOAA/OLE WEST COAST DIVISION	DAPS
9/4/2025	DPS-739442	U.S. ATTORNEY'S OFFICE	DAPS
9/4/2025	DPS-783255	U.S. DEPARTMENT OF HOMELAND SECURITY, FEDERAL PROTECTIVE SERVICE, RAPID PROTECTION FORCE	DAPS
9/4/2025	DPS-825884	U.S. DEPT OF HOMELAND SECURITY, CBP-INTELLIGENCE	DAPS
9/4/2025	DPS-513211	U.S. ENVIRONMENTAL PROTECTION AGENCY – CRIMINAL INVESTIGATION DIVISION	DAPS
9/4/2025	DPS-808709	U.S. SECRET SERVICE-SPOKANE	DAPS
9/4/2025	DPS-147913	U.S. TREASURY DEPT/INSPECTOR GENERAL	DAPS
9/4/2025	DPS-759680	US CUSTOMS AND BORDER PROTECTION – OFFICE OF PROFESSIONAL RESPONSIBILITY, CBP-OPR	DAPS
9/4/2025	DPS-506040	US DEPARTMENT OF VETERANS AFFAIRS POLICE – VANCOUVER VA MEDICAL CENTER	DAPS
9/4/2025	DPS-771030	US NAVY, REGION LEGAL SERVICE OFFICE NORTHWEST, BRANCH OFFICE WHIDBEY ISLAND	DAPS
9/4/2025	DPS-867116	VETERAN AFFAIRS PD	DAPS

Many eservice accounts associated with certain entities have maintained compliance with all contractual requirements, including their annual attestation, and have not demonstrated any violations of state law. Table 5 shows these active accounts as of May 2026.

Table 5. Active accounts

Account number	Agency name	Service
DPS-611443	AIR FORCE, DEPT OF, 82D SECURITY FORCES SQUADRON	DAPS
DPS-838444	BUREAU OF ALCOHOL, TOBACCO, FIREARMS/SEATTLE	DAPS
DPS-787068	COAST GUARD INVESTIGATIVE SERV	DAPS
DPS-787599	DEA BELLINGHAM	DAPS
DPS-805500	DEA SEATTLE	DAPS
DPS-846364	DEA YAKIMA	DAPS
DPS-490867	DEA/TNET	DAPS
DPS-619635	DEFENSE CRIMINAL INVESTIGATIVE SERVICE	DAPS
DPS-716270	ENERGY, DEPT OF RICHLAND OPERATIONS	DAPS
DPS-688487	FBI – SEATTLE	DAPS
DPS-683502	FEDERAL MOTOR CARRIER SAFETY ADMINISTRATION	DAPS
DPS-672103	INTERNAL REVENUE SERVICE	DAPS
DPS-907514	JBLM YAKIMA TRAINING CENTER POLICE DEPT.	DAPS
DPS-848684	JOINT BASE LEWIS-MCCHORD POLICE	DAPS
DPS-627827	NCIS NORTHWEST FIELD OFFICE	DAPS
DPS-684391	NORTHWEST HIDTA	DAPS
DPS-731886	OLYMPIC NATIONAL PARK	DAPS
DPS-449711	U.S. ARMY, CRIMINAL INVESTIGATION COMMAND	DAPS
DPS-083106	U.S. FOOD AND DRUG ADMINISTRATION, OFFICE OF CRIMINAL INVESTIGATIONS	DAPS
DPS-507505	U.S. GENERAL SERVICES ADMINISTRATION, OFFICE OF INSPECTOR GENERAL	DAPS
DPS-797308	U.S. MARSHALS SERVICE, SEATTLE	DAPS
DPS-599155	U.S. MARSHALS SERVICE, SPOKANE	DAPS
DPS-498145	U.S. POSTAL INSPECTION SERVICE	DAPS
DPS-783503	U.S. SECRET SERVICE-SEATTLE	DAPS
DPS-695790	U.S. SMALL BUSINESS ADMIN, OFFICE OF INSP GENERAL,	DAPS
DPS-724462	USDA FOREST SERVICE	DAPS
DPS-791004	USDA FOREST SERVICE MT. BAKER – SNOQUALMIE NATIONAL FOREST	DAPS
DPS-801585	VETERANS AFFAIRS, OFFICE OF INSPECTOR GEN	DAPS

How DAPS customers demonstrate compliance

Under the terms of the DAPS data sharing agreement, authorized account administrators are required to conduct annual self-assessments of their users' compliance with the agreement, including prohibitions on the use of DOL data or systems for civil immigration enforcement. Specifically, article 9 of the agreement provides:

> Data may only be used for lawful actions related to the Licensee's functions as a governmental agency, and as directly related to the purposes set forth in Licensee's application, and as approved by DOL. All other use of Data is strictly prohibited. DOL further retains the right to re-determine its approval for permitted uses and may cancel or restrict such uses at a later date if such uses do not comply with state law or DOL policy. If any purposes noted in the application are otherwise restricted by any terms of this Agreement, then the restrictions herein are controlling. This prohibition on certain uses includes, without limitation, the use of Data for purposes of investigating, locating, or apprehending individuals for immigration related violations.

Each DAPS and DIAS customer must report on their compliance obligations to DOL using a standard form, reproduced below as Figure 5. DOL's Data-Management Office collects, reviews, and retains these forms as evidence of compliance.

WASHINGTON STATE DEPARTMENT OF LICENSING

E-Services Annual Statement of Compliance

Service contract holders use this form to certify their compliance as required in their agreement with the Department of Licensing (DOL). Failure to submit this certification may result in DOL conducting an audit at your expense, suspension of service, or termination of the agreement.

Email this completed form to DataServices@dol.wa.gov. If you are sending information that includes data privacy and security deficiencies or other sensitive information, contact DataServices@dol.wa.gov for a secure email link.

Agency information

Agency name		E-Services Account ID number, if applicable
E-Services account type ☐ DAPS ☐ DIAS ☐ AVR ☐ DRR		
Contact name	10-digit phone number	Email
Authorized signer name	10-digit phone number	Email

Privacy and Security Requirements and annual statement of compliance

The evaluation must include:

- Review and verification of the Privacy and Security Requirements in your agreement.
- Review of all authorized users' access and use of Protected Personal Information to make sure their access and use is within official job duties and the permissible uses in your agreement.
- Institute and maintain written policies and procedures to ensure data is used only as authorized in the contract.
- Require authorized users to sign an Appropriate Use Declaration prior to accessing an E-Service through License eXpress.

Answer the following

1. Did you conduct your annual self-assessment? . . . . . ☐ Yes ☐ No
   If "No," why not?

2. Are you in compliance with the Privacy and Security Requirements? . . . . . ☐ Yes ☐ No
   If "No," describe any deficiencies and what has been done to resolve them:

3. Did you review all authorized users' access and revoke access when it was no longer required? ☐ Yes ☐ No
   If "No," explain:

4. Did you have any security breaches or unauthorized use of DOL data? . . . . . ☐ Yes ☐ No
   If "Yes," describe the breaches or violations and what has been done to resolve them:

By typing or signing your name, you declare under penalty of perjury under the law of Washington that the foregoing is true and correct.

Date and place (city or county) signed

X
Authorized signature

DSC-425-005 (R/11/25)EA

Figure 5. E-Services Annual Statement of Compliance

Implementing Executive Order 25-09

Governor Ferguson's Executive Order 25-09: Reaffirming Washington's Commitment to Protecting the Rights and Interests of Immigrant Communities, requires agencies to take certain measures to enhance data privacy and security, including the following:

- Effective immediately, and consistent with the values set forth above, all cabinet agencies shall continue to review their data collection, sharing, and retention policies to ensure they are treating the protection of residents' personal and private information as a matter of public interest and safety.
- All cabinet agencies, boards, and commissions shall continue to follow closely any guidance from the Attorney General's Office and the Office of Privacy and Data Protection regarding their data collection, sharing, and retention practices.
- Cabinet agencies shall continue to consult with the Attorney General's Office and the Office of Privacy and Data Protection to ensure that the benefits and potential risks of any data collection, sharing, or retention not strictly required by law or critical to state interests are carefully considered with the goal of protecting residents' privacy and safety.
- Consistent with any guidance received from the Attorney General's Office and the Office of Privacy and Data Protection, and in accordance with state and federal law, cabinet agencies, boards, and commissions shall continue to consider and make any changes to their data collection, sharing, and retention practices that may be appropriate to ensure they are treating the protection of residents' personal information as a matter of public interest and safety.
- In accordance with the above guidance and the processes set forth in this Executive Order, cabinet agencies should work to communicate any potential risks to residents' data quickly, proactively, and in a format and language that is accessible for the recipient.
- In the performance of the above duties, cabinet agencies should remain mindful and respectful of the principles of tribal and indigenous data sovereignty in connection with the collection, storage, and sharing of any information regarding tribal citizens and nations.[3]

The Department of Licensing continues to review its data collection, sharing, and retention policies to ensure they are treating the protection of residents' personal and private information as a matter of public interest and safety. The agency routinely seeks and follows guidance from the Governor's Office, the Attorney General's Office and the Office of Privacy and Data Protection. The agency continues to communicate any potential risks to residents' data quickly and proactively.

[3] governor.wa.gov/sites/default/files/exe_order/25-09%20-%20Protecting%20Immigrant%20Communities%20%28tmp%29.pdf

In addition to the review and consultations described above, the agency also participates actively in the Immigration Subcabinet established by Executive Order 25-09 and draws upon the insights and opportunities provided by DOL's PEAR Impact Team to evolve protections for vulnerable and concerned communities.

Immigration Subcabinet

The Department of Licensing is an active participant in the Immigration Subcabinet, with agency leaders participating in both the policy and the data committees.

The data committee works to make Washington's data systems more just and effective so everyone, especially immigrants, LGBTQ+ people, and people with disabilities, is seen, protected, and served fairly. The group aims to do this by improving data quality, privacy, and community voice in decision making to ensure policies lead to real-world impact and equitable outcomes. This committee guides the Immigration Subcabinet in developing statewide standards and practices that build trust, improve representation, and strengthen accountability in how data is collected, shared, and used to inform public policy.

PEAR Impact Team

Since 2022, the Department of Licensing has had a robust and engaged team focused on ensuring it is effectively serving all Washingtonians. This team, now called the DOL PEAR Impact Team, has had a membership of 50 to 60 members since 2024 and aims to honor internal and external partners. DOL's partners recommend solutions and serve as informal ambassadors of DOL to the communities of which they're a part.

Between November and December 2025, PEAR Impact Team staff in DOL's Equity and Inclusion Office met individually with every PEAR Impact Team member. Based upon those conversations, PEAR Impact Team members developed a ranking survey of the priority populations, needs, and recommended work for 2026. Those results conveyed a prevailing theme of protecting people and data. The team identified immigrants, refugees, and asylees as the community with the most urgent needs from DOL.

At its March 2026 meeting, the PEAR Impact Team called on the agency's privacy officer to present and be accountable to the group regarding agency training for protecting privacy and data. The group reviewed and discussed the agency's mandatory privacy and data protection training for new employees.

Part B. DAPS and DIAS Statistical Reporting

There are currently 730 accounts of all types associated with DAPS and DIAS. Most belong to Washington municipal or county governments and are split about evenly between law enforcement and courts. Figure 6 below shows the distribution of DAPS and DIAS accounts by the domain of the customer (courts, attorneys, law enforcement, etc.) and the type of jurisdiction (municipal, county, state, tribal, and federal).

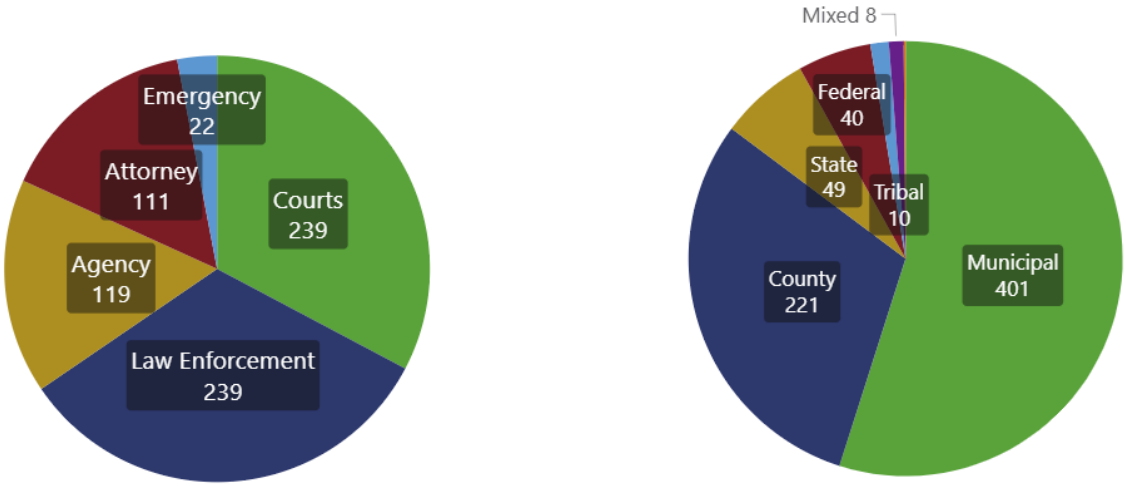


Figure 6. DAPS and DIAS accounts by jurisdiction and domain

Queries of the DAPS and DIAS systems vary somewhat from month to month, as indicated by the chart in figure 7 below, covering the quantities of queries during the first quarter of calendar year 2026.

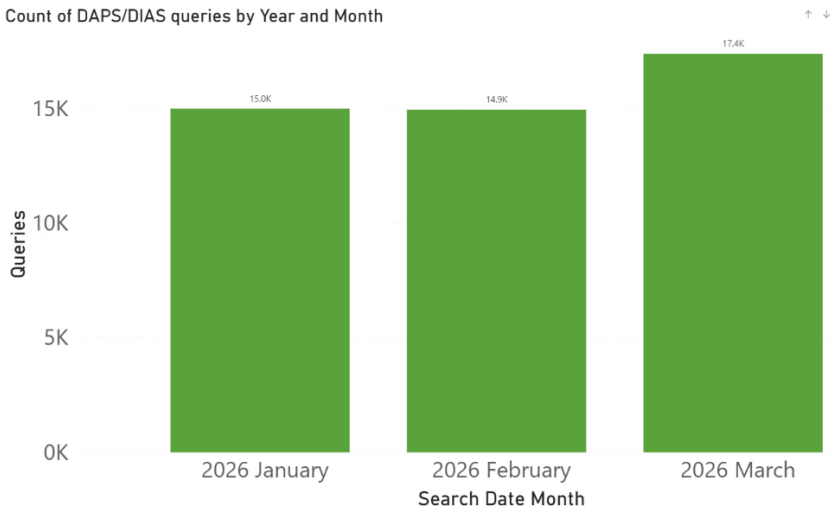


Figure 7. Total DAPS and DIAS queries per month

The most active users of the DAPS and DIAS systems remain fairly consistent over time. Organizations such as the Department of Revenue, the Department of Children, Youth and Families, the FBI, and the Seattle Police Department are routinely among the top ten monthly users of these systems, as shown in Figure 8.

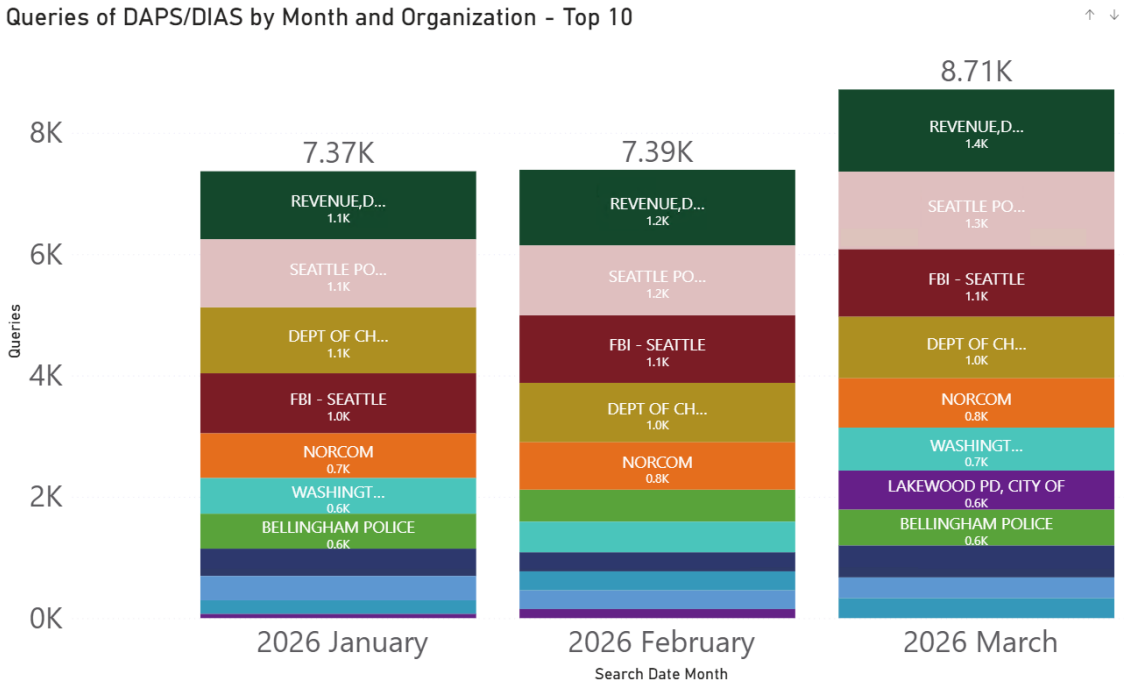


Figure 8. Top 10 organizations querying DAPS and DIAS

The data for this recurring report

In order to comply with the schedule provided by law, this report was compiled using only existing staff, reporting tools, and data. Future reports might include corrections and new analysis once the resources made available by the Legislature for this purpose are available during fiscal year 2027, which begins July 1, 2026.

In the future, DOL intends to use a portion of the resources provided by the Legislature for these quarterly reports to publish the raw data compiled here as an open dataset on the state's open data portal, data.wa.gov.[4] On this open data portal, the agency already publishes a variety of documented and verified data on topics such as vehicle registrations, professional licenses, electric vehicle population, and driver licenses and ID cards transferred to Washington. Interested parties should then be able to analyze for themselves the same statistical and summary data used by the agency for this and future

[4] data.wa.gov/browse?q=department%20of%20licensing

reports. Information likely to identify specific people will be either redacted or not included at an individualized level.

Part C. ACCESS and Nlets Statistical Reporting

What is Nlets?

Nlets is a 501(c)(3) organization. The FBI controls which entities have access to Nlets. Washington state (through the Washington State Patrol) is an Nlets user, in addition to all other states and territories, local jurisdictions, certain Canadian jurisdictions, Interpol, and federal agencies.

Nlets allows law enforcement and criminal justice agencies access to various driver, vehicle, and law enforcement databases maintained by federal, state, and local agencies. Unlike DAPS, Nlets doesn't allow for search terms with expanders. In the case of a driver record query, the user must know the individual's full name and date of birth in order to obtain the record. WSP has an interface called ACCESS that allows DOL driver and vehicle data, law enforcement data, and other data sources to be used by Washington-based law enforcement only. Select Washington data flows into Nlets for use by broader Nlets users.

Washington state has the ability to prohibit data from reaching certain users through Nlets through WSP's ACCESS interface. Washington state has cut off access to DOL data through Nlets for:

- ICE — Enforcement and Removal Operations (ERO)
- ICE — Homeland Security Investigations (HSI)

DOL shares the following data fields through Nlets:

- Full name
- Date of birth
- Driver license number
- Address
- Physical identifying features (height, weight, eye color)
- Driving status – restrictions and endorsements
- Vehicles/license plates/VIN numbers
- Photo from driver license (Nlets only)

Nlets data and statistics

As required by Proviso 31, DOL has begun collecting statistical information from the ACCESS and Nlets systems for queries of the DOL DRIVES system. This data is largely new to DOL because the ACCESS system is owned and managed by the Washington State Patrol. Once fiscal year 2027 funds provided by the budget become available as of July 1, 2026, DOL intends to study the ACCESS/Nlets data and include analysis in the second quarterly report, planned for September 2026. If feasible and appropriate, DOL also intends to publish anonymized data for independent analysis.

Part D. Appendix A and Glossary of Terms

DOL goal setting and strategies

DOL takes protecting customer data seriously. The agency's past experience has provided an opportunity to improve the data-management and data-privacy infrastructure to better protect customers' data. DOL has made this an agency strategic plan priority and a priority for internal data governance.

DOL's strategic plan for 2021 to 2025 described key goals and objectives for transforming our approach to data. They're reproduced in Figure 1 below and described in the text that follows.

Figure 1. 2019 Strategic plan safer data

Additionally, DOL is incorporating a data protection goal into its latest version of the strategic plan, which is currently under development.

In attaining the agency's strategic plan goals since 2019, DOL has adopted and implemented a data governance framework using the policies and standards listed in Table 1 below.

Table 1. Data governance policies and standards

Policy/Standard	Number
Data ethics	1.7.12
Data governance	1.7.6
Structured data: Roles and responsibilities	1.7.7
Structured data: Access and release	1.7.8
Data privacy: Employee responsibility to protect the privacy of data	1.7.1
Data privacy: Data service requests and external requests for sensitive and confidential information	1.7.9
Data privacy: Driver and vehicle data systems access	100.03.01
Release of security information for and samples of driver licenses	600.200.01
Data classification standard	
Data handling standard	
Active directory documentation standard	
Information request analysis standard procedure	

In addition to the policies and standards described above, DOL's Data-Management Office added language from the Keep Washington Working Act into its data sharing agreements and developed a compliance audit program for DOL's largest data customers, including:

- Data security requirements (NIST 800-63/ISO27001 or State Auditor's Office (SAO) Agreed-upon Procedures).
- In-depth audits of each bulk data recipient's use of our customers' data, conducted by DOL staff once every three years.

Table 2 shows the number of audits conducted on DOL's bulk data customers since 2018, including data brokers like Lexis-Nexis, state agencies like the WA Department of Revenue, and local governments like the City of Vancouver. Currently, DOL has approximately 100 of these high-volume or bulk data sharing partner relationships.

Table 2. Audits of bulk data recipients, 2018 to 2026

Year	Audits
2018	9
2019	19
2020	13
2021	12
2022	28
2023	46
2024	26
2025	26
2026 (YTD)	11
Total	190

In 2019, DOL formed a new team of professional data stewards. This team has developed and delivered a curriculum of regularly refreshed general and topic-specific privacy and data literacy training. The agency's training commitments include a specific mandatory course on the Keep Washington Working Act, which has been completed by 1,356 DOL employees (99 percent of staff), and data literacy training for specific roles. Figure 2 is a sample screen from the Keep Washington Working Act.

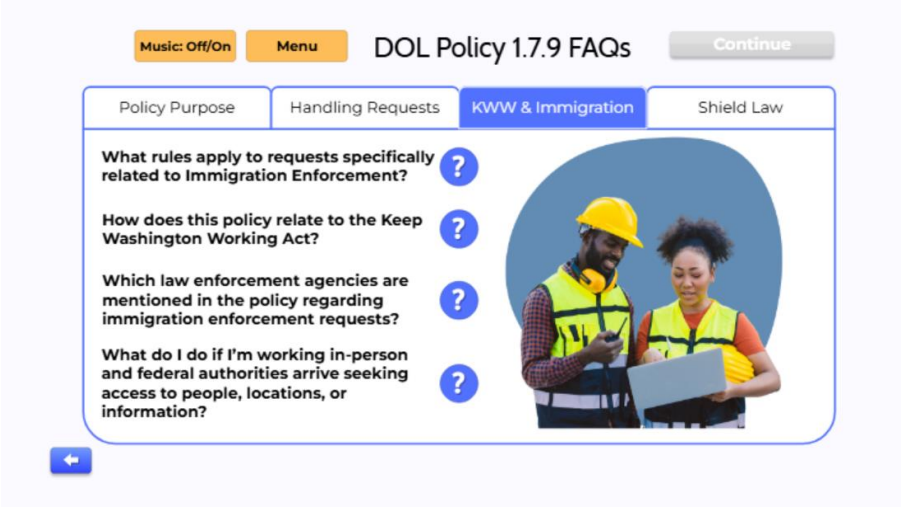


Figure 2. Screen from Keep Washington Working training

DOL's data stewards have also developed role-specific data literacy training, known as the Data Wilderness Camp, for a variety of roles within the agency. A sample overview screen

from one of these courses is provided below as Figure 3. These courses are delivered using a mix of live and self-paced modules adapted for roles such as analysts or leaders. We have shared DOL's Data Wilderness Camp training with other Washington state agencies.

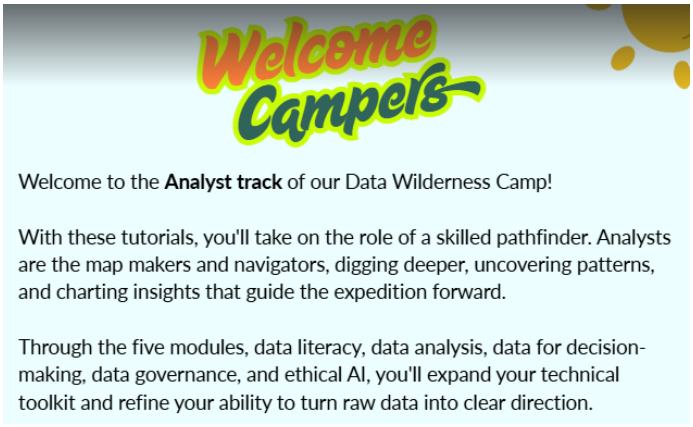


Figure 3. Role-specific data literacy training — Data Wilderness Camp overview

Website Privacy center and privacy notice

DOL's Privacy center webpages[5] (see Figure 4) have expanded along with the agency's privacy program. Through these webpages DOL has addressed common questions and concerns. The agency is also proactively transparent about data recipients, revenue from data sales, and other privacy topics of interest. DOL uses these pages as the agency's privacy notice, informing customers about the information collected, its use, and their rights in the data DOL holds.

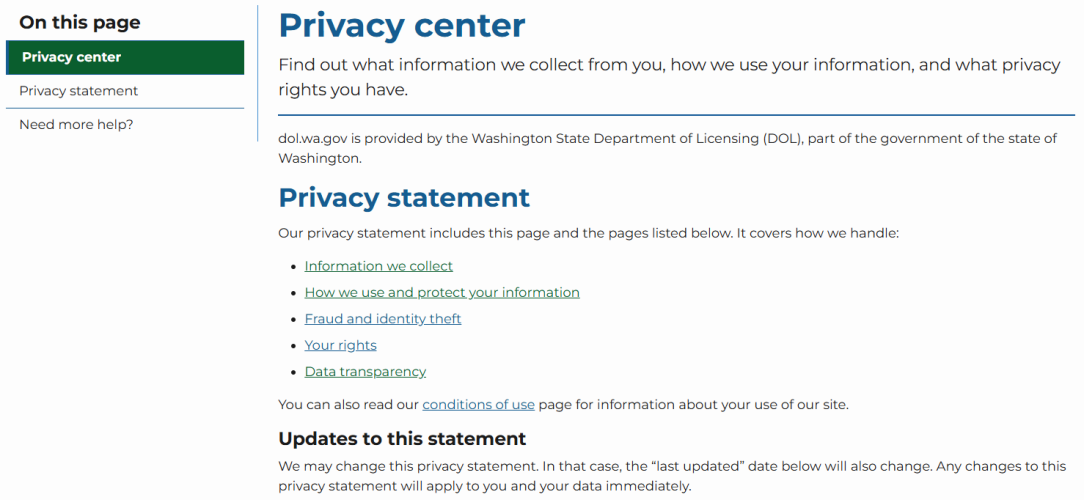


Figure 4. DOL website Privacy center

[5] dol.wa.gov/about/privacy-center

Glossary of Terms

- **ACCESS.** Washington State Patrol's "A Central Computerized Enforcement Service System." This is the interface that connects Washington's state and local law enforcement and criminal justice agencies to driver, identity, and criminal history databases from around the country.
- **DAPS.** DOL's "Driver and Plate Search." This is a search tool built by DOL and made available to law enforcement agencies that access driver and vehicle data. The tool has better search functionality than ACCESS or Nlets, allowing the user to search incomplete names or partial license plate numbers.
- **Database.** A set of data held by an entity. DOL maintains databases with its customers' information. If certain data is made available to a user or a set of users within an interface, it is done so with specific permissions and appropriate limitations. For example, Nlets and ACCESS users pull limited data from DOL's driver and vehicle databases.
- **Data sharing agreement.** A contract with external entities that governs the protection and authorized uses of Department of Licensing information. The agreement contains terms and conditions as required by statute (RCW 46.22.010), rule (Chapter 308-10A WAC), policy (WaTech Data Sharing Policy SEC-08 or DOL Data Privacy 1.7.9), and best practices for security and privacy.
- **DIAS.** DOL's Driver Information and Adjudication System. A web-based query system used to view or electronically update driver records, enter formal judgments on driver records, and to process various court related forms. See Driver Information and Adjudication System (DIAS) Guide.
- **DRIVES.** DOL's system for identity, driver, and vehicle licensing and registration transactions and their corresponding records.
- **Eservices.** Services offered by DOL that allow certain types of customers to complete tasks related to Washington driver or vehicle data using a standard web browser. Most eservices are designed for businesses or government agencies that have frequent and legally authorized needs to search for, copy, or modify DOL data. Eservices are distinct from bulk data services, which require more technical skill or special tools.
- **Identicard.** A card issued by the Department of Licensing that can be used to prove the identity of the holder but doesn't establish the holder's qualifications as a driver of a motor vehicle. See RCW 46.20.117.

- **Interface.** This is the technology used to connect multiple systems and databases. An interface does not necessarily have data or records of its own.
- **Nlets.** The International Justice and Public Safety Network (Nlets) connects all 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, and Canada to enable a secure exchange of criminal justice data. Nlets gives users access to various driver, vehicle, and law enforcement databases maintained by federal, state, and local agencies. It has been in existence since 1970.
- **Permissible Use Audit.** An independent assessment of the controls in place to protect the privacy of personal information and ensure the auditee is using personal information in accordance with the requirements imposed in a data sharing agreement.