PUBLIC-RECORD SAMPLE

Washington ALPR Governance Review

Tacoma Police Department

A demonstration of the evidence, findings, and implementation tools included in an ALPR Governance review.

REVIEW BASIS	PUBLIC RECORDS AVAILABLE THROUGH SEPTEMBER 15, 2026
PRIMARY LAW	ESSB 6002 | CHAPTER 239, LAWS OF 2026
SYSTEM IDENTIFIED	AXON MOBILE ALPR | 242 DASHCAM-INTEGRATED UNITS
PUBLIC STATUS	JUNE NOTICE: INACTIVE PENDING COMPLIANCE WORK

This sample uses public documents to show the review method. It does not state Tacoma's current compliance posture, evaluate nonpublic records, or replace agency counsel or the agency's required internal audit.

Prepared by ALPR Governance | A service of Fugal Foundry LLC

01 | EXECUTIVE ASSESSMENT

A documented program transition is still visible in the public record.

Tacoma's June 1 notice describes a 242-unit Axon mobile ALPR deployment as inactive and states that the system, policy, and training still required changes for ESSB 6002. The Attorney General's public index later lists a Tacoma registration dated July 8, 2026. The records available for this sample do not show the later configuration, policy text, training revisions, or audit-trail controls.

7	priority policy or procedure actions	7	items requiring internal evidence	2	future statutory milestones	1	item for focused counsel review

Overall sample finding

The public record shows a responsible pause and an explicit plan to modify the program. Before activation, the agency should be able to demonstrate that its current policy, system settings, vendor controls, training, audit records, and approved registration all reflect ESSB 6002. The June policy attached to the notice does not yet provide that evidence.

What is already documented

01	**Named responsibility**	Policy 426 assigns ALPR administration, retention, and access responsibility to the Administrative Services Bureau Commander.
02	**Training requirement**	The policy requires approved training before operation or access, and the notice states that a documented training process exists.
03	**Activity logging**	The policy requires a protected system capable of recording access by name, date, and time.
04	**Public transition record**	The June notice identifies the vendor, deployment type, unit count, inactive status, program contact, and outstanding compliance work.

02 | PRIORITY ACTION PLAN

Resolve the visible conflicts before relying on the current policy.

These actions are prioritized from public documents. A full engagement would validate them against the agency's current policy, approved registration, vendor settings, training material, and audit exports.

01

Replace the 30-day default retention rule

Finding: Policy 426 states that all ALPR data is stored for 30 days unless needed for an active investigation. ESSB 6002 establishes a 21-day general limit with specific exceptions.

Action: Set the default to no more than 21 days, document each exception, define the deletion trigger, and validate the setting in Axon.

Likely owner: Program administrator + records + vendor

02

Narrow authorized uses

Finding: The policy permits official law-enforcement business, patrol operations, and department investigations. The statute authorizes a narrower set of enumerated purposes.

Action: Rewrite the permitted-use section around the statutory categories and align search-purpose selections, training, and supervisor review.

Likely owner: Counsel + policy owner + training

03

Make alert verification mandatory

Finding: The policy says officers should verify an alert through ACCESS 'if practicable.' The statute requires independent reasonable suspicion or immediate visual and database confirmation before a stop.

Action: Replace discretionary language with the statutory decision rule and add it to operator training and supervisory review.

Likely owner: Patrol operations + training

04

Define restricted locations and purposes

Finding: The public policy does not address the statute's protected facilities or prohibitions involving immigration enforcement, protected health care, and constitutionally protected activity.

Action: Add operational controls, placement review, documented exceptions, and escalation steps for restricted locations and prohibited purposes.

Likely owner: Counsel + program administrator

02 | PRIORITY ACTION PLAN CONTINUED

Complete the governance controls around access, evidence, and review.

05

Reconcile sharing and direct access

Finding: Policy 426 permits release to authorized and verified law-enforcement officials and agencies at any time for legitimate purposes. ESSB 6002 uses more specific rules for disclosure, sharing, and direct access.

Action: Have counsel map each existing sharing relationship and workflow to the statute, then configure vendor permissions and approval rules to match.

Likely owner: Counsel + program administrator

06

Expand audit-trail requirements

Finding: The policy requires name, date, and time. The statute also requires query elements, purpose and offense type, case or call number, camera location, export/download/share activity, and available vendor audit records.

Action: Confirm that each required field is captured, exportable, retained by the agency for two years, and protected from investigative reuse.

Likely owner: Program administrator + IT + vendor

07

Formalize the annual internal audit

Finding: The public policy says audits should occur on a regular basis. The law requires at least one internal audit each year covering access, use, retention, purging, sharing, and agency policy.

Action: Adopt an annual procedure, assign an independent reviewer, define sampling and exception handling, and preserve evidence of completion.

Likely owner: Chief's designee + internal reviewer

Activation gate

Before any unit returns to service, retain a signed readiness record showing approved registration, current policy, completed training, validated settings, authorized user list, vendor controls, audit-export capability, and leadership approval.

03 | REQUIREMENT MATRIX

Program authority and data handling

Status reflects only the public evidence reviewed. 'Evidence needed' means the control may exist but could not be validated from the reviewed documents.

REQUIREMENT	PUBLIC-RECORD OBSERVATION	STATUS	NEXT STEP
Registration	The June notice expressed intent to register. The Attorney General's public index lists Tacoma Police Department with a July 8, 2026 registration.	EVIDENCE NEEDED	Retain the approved form, acceptance record, certification, and current system inventory.
Policy in effect	Policy 426 exists, but the copy attached to the June notice predates the new law and the notice says it required modification.	ACTION NEEDED	Approve and publish the revised policy before activation.
Training process	The notice states that a documented process exists and would be modified. Training records were not reviewed.	EVIDENCE NEEDED	Obtain curriculum, completion records, refresher cadence, and acknowledgment forms.
Authorized purposes	Policy language extends to general official business, patrol operations, and department investigations.	ACTION NEEDED	Map policy language and system purpose codes to the statute's enumerated uses.
Prohibited purposes	No explicit prohibition was located for immigration enforcement, protected health care, or protected constitutional activity.	ACTION NEEDED	Add explicit prohibitions and supervisor escalation procedures.
Restricted locations	No control was located for protected health care facilities, immigration facilities, schools, worship sites, courts, or food banks.	ACTION NEEDED	Inventory camera capture areas and document placement and access controls.
Data ownership	The public policy does not state that the agency is the legal owner of data collected by its system.	ACTION NEEDED	Add ownership language and confirm the vendor contract reflects it.
Alert response	Policy says ACCESS verification should occur 'if practicable' before enforcement based solely on an alert.	ACTION NEEDED	Replace with the mandatory statutory verification rule.
General retention	Policy sets 30 days. The statute sets a 21-day general maximum.	ACTION NEEDED	Revise policy, settings, purge evidence, and exception logging.

03 | REQUIREMENT MATRIX CONTINUED

Vendor controls, audit evidence, and public accountability

REQUIREMENT	PUBLIC-RECORD OBSERVATION	STATUS	NEXT STEP
Retention exceptions	The policy references active investigations and the records schedule but does not map the statute's exception categories and deletion triggers.	ACTION NEEDED	Create exception categories with authority, owner, review date, and deletion event.
Sharing and access	The policy allows release to verified law-enforcement agencies for legitimate purposes; the statute is more specific and should be reconciled by counsel.	COUNSEL REVIEW	Inventory all direct access, sharing, networks, and judicial-disclosure workflows.
Database updates	No evidence reviewed shows required databases are checked for updates at least every 24 hours.	EVIDENCE NEEDED	Obtain vendor configuration and monitoring evidence.
Vendor controls	The June notice states that vendor modification was still under discussion. Current technical controls were not reviewed.	EVIDENCE NEEDED	Obtain a vendor control attestation and configuration export.
Change consent	No public evidence shows controls requiring agency knowledge and explicit consent before vendor changes affecting sharing.	EVIDENCE NEEDED	Document the change-control and consent workflow in contract and procedure.
Audit trail fields	Policy requires name, date, and time but does not enumerate the full statutory field set.	EVIDENCE NEEDED	Test a current export against every field in Section 8(1).
Two-year audit retention	No public evidence confirms that agency-held audit-trail data and vendor records are retained for two years.	EVIDENCE NEEDED	Define storage, export cadence, integrity checks, access, and deletion.
Annual internal audit	Policy says audits 'should' occur regularly; scope and annual cadence are not defined.	ACTION NEEDED	Adopt the annual procedure and assign the reviewing role.
Public awareness	The June notice states that measures had been or would be taken before implementation. Supporting evidence was not reviewed.	EVIDENCE NEEDED	Retain council materials, public notice, web publication, or equivalent evidence.

03 | REQUIREMENT MATRIX CONCLUSION

Future milestones need current data collection.

The annual report is due beginning December 1, 2027, but several fields require cumulative counts. Waiting until the reporting deadline would create a preventable reconstruction problem.

REQUIREMENT	PUBLIC-RECORD OBSERVATION	STATUS	NEXT STEP
Policy-change notice	Beginning after December 1, 2026, policy changes or repeal require notice and copies to the Attorney General within 60 days.	FUTURE MILESTONE	Add the notice to policy change control and assign ownership.
Model-policy alignment	By December 1, 2027, agencies must adopt a policy consistent with the Attorney General model or explain departures.	FUTURE MILESTONE	Plan a formal gap review after the model policy is published by July 1, 2027.
Annual public report	The public policy predates the required report fields and does not assign collection or publication responsibility.	FUTURE MILESTONE	Begin collecting each required metric now; assign owner and validation process.

Status legend

ALIGNED	Public evidence directly supports the requirement.
ACTION NEEDED	Public evidence shows a visible conflict or missing policy element.
EVIDENCE NEEDED	The control may exist but requires internal evidence.
COUNSEL REVIEW	The statute and current workflow require legal interpretation.
FUTURE MILESTONE	A dated obligation requires present preparation.

Important reading rule

An 'evidence needed' rating is not a finding of noncompliance. It identifies a question that cannot be closed from public documents and should be resolved during the agency review.

04 | EVIDENCE REQUEST

The documents needed to complete the review

A customer review begins with a focused evidence request. The agency can answer many questions with configuration summaries and governance records without transferring license plate numbers, vehicle images, or investigative search data.

EVIDENCE REQUEST CHECKLIST

- Approved Attorney General registration form, submission confirmation, and current inventory of vendors, units, deployment types, and locations.
- Current adopted and published ALPR policy, related location-tracking policy, general access-control standards, and relevant records schedule.
- Current vendor contract, data-processing terms, sharing permissions, change-control terms, and vendor compliance or control attestations.
- Screenshots or exports showing retention, sharing, access roles, purpose codes, case-number requirements, alert settings, and purge configuration.
- Training curriculum, operator and administrator completion records, refresher schedule, and policy acknowledgment records.
- Current authorized-user list, role assignments, approval and termination procedures, and periodic access review evidence.
- De-identified audit export or data dictionary showing every available field, plus the agency's vendor-export and two-year retention process.
- Internal audit procedure, completed audit evidence if available, exception findings, remediation records, and leadership sign-off.
- Inventory of data-sharing and direct-access relationships, judicial disclosure workflow, preservation requests, and court-order tracking.
- Public awareness materials, website policy link, council or governing-body materials, and existing usage metrics for annual reporting.

Data minimization

For this document-based review, sensitive ALPR event data remains with the agency. If audit-log validation is added, query elements should be masked or de-identified while preserving the fields needed to test completeness and process controls.

05 | INTERNAL AUDIT TOOLKIT

A repeatable procedure for the agency's annual review

ESSB 6002 assigns the internal audit to the agency. This procedure organizes that work and its evidence. The agency selects the reviewer, approves the scope, resolves exceptions, and issues the result.

STEP	CONTROL	AUDIT PROCEDURE
01	**Freeze the review period**	Identify the dates, systems, units, users, and vendor environments covered. Preserve the relevant logs before analysis.
02	**Reconcile access**	Compare authorized users and roles against active accounts, personnel status, training completion, and least-privilege assignments.
03	**Test audit completeness**	Confirm required fields are populated and agency-held vendor records cover the full review period without unexplained gaps.
04	**Review searches and access**	Use a documented sampling method or complete review. Test authorized purpose, case or call number, offense type, and approvals.
05	**Review exports and sharing**	Reconcile downloads, exports, direct-access relationships, judicial disclosures, and exceptions against agency policy and law.
06	**Test retention and purging**	Validate default settings, samples near the deletion boundary, exceptions, preservation authority, and final deletion events.
07	**Record and remediate exceptions**	Assign owner, priority, target date, and evidence of closure. Escalate potential violations through the agency's approved process.
08	**Approve and preserve the result**	Obtain reviewer and leadership sign-off, retain supporting evidence, and route required results into annual reporting.

05 | INTERNAL AUDIT WORKSHEET

Exception log and sign-off

The production deliverable includes a reusable worksheet. This sample shows the fields that preserve accountability from discovery through closure.

ID	DATE	SYSTEM / USER	REQUIREMENT	EXCEPTION	PRIORITY	OWNER	DUE	CLOSED
E-01								
E-02								
E-03								
E-04								
E-05								
E-06								
E-07								

Review sign-off

REVIEW PERIOD		SYSTEMS COVERED	
REVIEWER		DATE COMPLETED	
PROGRAM OWNER		LEADERSHIP APPROVAL	

06 | PUBLIC REPORTING READINESS

Build the December 2027 report as data is created.

The statute identifies nine annual-report categories. The agency should assign a source system, owner, validation rule, and collection cadence for each field before operations begin.

REPORT FIELD	LIKELY SOURCE	OWNER	READINESS ACTION
Traffic stops / arrests / prosecutions	CAD, RMS, prosecutor disposition	Operations + records	Define ALPR-assistance flag and prosecution handoff.
Stolen vehicles / plates recovered	RMS case outcomes	Crime analysis	Use a consistent recovery attribution rule.
Preservation requests / disclosure orders	Legal and records tracking	Counsel + records	Log receipt, authority, scope, and disposition.
External access / sharing	Vendor and agency audit logs	Program administrator	Identify each governmental entity and count events.
Judicial-warrant access / sharing	Warrant and disclosure records	Counsel + records	Link each event to judicial authority.
Policy changes	Policy management system	Policy owner	Track effective date and effect on collection, retention, access, or sharing.
Internal audit results	Annual audit package	Assigned reviewer	Approve a public summary and preserve detailed evidence.
Reads / searches with results / alerts	Vendor metrics and audit export	Program administrator	Define counts and reconcile vendor totals.
Camera locations	Asset and deployment inventory	Program administrator	Maintain publishable location data for fixed and mobile systems.

Recommended cadence

Reconcile the underlying counts quarterly. This reduces year-end reconstruction work and gives leadership time to correct inconsistent definitions or missing fields before the public report is due.

07 | IMPLEMENTATION ROADMAP

A 90-day path from public gaps to documented readiness

The schedule begins when leadership confirms that the program will proceed. Activation timing remains an agency decision based on completed legal, policy, technical, and training work.

DAYS 1-30

- Confirm current approved registration and complete system inventory.
- Approve policy changes for retention, permitted uses, alert response, restricted locations, sharing, and internal audit.
- Obtain the current vendor control package and map every statutory audit field.
- Assign owners for training, access administration, annual audit, and public reporting.

DAYS 31-60

- Configure retention, purpose codes, required case numbers, roles, sharing, alerts, and vendor change controls.
- Complete operator and administrator training under the revised policy.
- Test purge behavior and export a de-identified audit sample for field completeness.
- Inventory direct-access and judicial-disclosure workflows with counsel.

DAYS 61-90

- Run a pre-activation audit using the approved internal procedure.
- Close or formally accept exceptions and preserve evidence of remediation.
- Complete the activation-gate record and leadership approval.
- Begin quarterly collection of the statutory annual-report metrics.

08 | METHOD, SOURCES, AND LIMITATIONS

What this sample establishes

This demonstration compares public agency records against the enacted statute and organizes visible gaps, evidence questions, and implementation work. It is intentionally candid about what the public record cannot establish.

Documents reviewed

1	**ESSB 6002, Chapter 239, Laws of 2026** Washington State Legislature. Enacted March 30, 2026. Sections 3 through 8 provide the primary operational, retention, sharing, policy, audit, and reporting requirements. https://lawfilesext.leg.wa.gov/biennium/2025-26/Pdf/Bills/Session%20Laws/Senate/6002-S.SL.pdf
2	**Tacoma notice of intent to register** Tacoma Police Department, June 1, 2026. Identifies the Axon mobile system, 242 units, inactive status, current policy and training, and pending compliance work. https://waspc.memberclicks.net/assets/legislative/APLR/Tacoma%20-%20ALPR%20AG%20Letter%20final.docx.pdf
3	**Tacoma Police Department Policy 426** Published policy attached to the June notice. The document bears a December 19, 2024 Lexipol copyright date and contains rules for use, retention, safeguards, audits, and training. https://waspc.memberclicks.net/assets/legislative/APLR/Tacoma%20-%20P426%20Automated%20License%20Plate%20Readers%20Tacoma%20Police.pdf
4	**WASPC ALPR Interim Guidance** Washington Association of Sheriffs and Police Chiefs, May 29, 2026. Operational guidance pending the Attorney General model policy. https://waspc.memberclicks.net/assets/legislative/APLR/WASPC%20ALPR%20Interim%20Guidance%20-%20Final.pdf
5	**Washington Attorney General registration index** Public index listing Tacoma Police Department with a July 8, 2026 registration date. The sample does not assume the content of the later submission. https://www.atg.wa.gov/automated-license-plate-reader-alpr-system-registration

Limitations

- No live system, configuration, contract, training record, access list, audit trail, search record, sharing record, purge evidence, internal audit, or nonpublic policy was reviewed.
- The July 8 registration listing confirms a later public event but does not, by itself, establish the content or current effectiveness of every program control.
- Findings describe the reviewed public documents as of September 15, 2026. Later agency action may resolve any item shown here.
- This is an operational governance assessment. It is not legal advice, a legal opinion, an attestation engagement, or a certification of compliance.

Production review

A paid engagement replaces public-record assumptions with agency-supplied evidence, validates the current program, documents exceptions, and delivers agency-specific audit and reporting tools.

WASHINGTON ALPR GOVERNANCE REVIEW

Know where the program stands. Know what happens next.

The $1,500 fixed-fee review converts policies, configurations, training records, contracts, and governance evidence into a requirement matrix, prioritized correction plan, internal-audit toolkit, and public-reporting readiness package.

INCLUDED	ENGAGEMENT	CONTACT
Agency-specific review Findings and action plan Audit and reporting tools	$1,500 one-time Fixed scope and fee Timing confirmed before work begins	fugalfoundry@gmail.com alprgovernance.com

ALPR Governance is vendor-independent. The review supports the agency's own governance and internal-audit work. Final legal conclusions remain with the agency and its counsel.