



STAFF REPORT TO THE CITY COUNCIL

DATE: Regular Meeting of August 25, 2026

TO: Honorable Mayor and Members of the City Council

SUBMITTED BY: Michael Mellone, Lieutenant

APPROVED BY: Joe Vigil, Chief of Police

SUBJECT: Adopt a Resolution Authorizing a Sole Source Agreement with Axon Enterprise, Inc. for Automated License Plate Recognition, In-Car Camera, and Integrated Public Safety Technology Systems

RECOMMENDED ACTION

It is recommended that the City Council adopt a resolution a sole source agreement with Axon Enterprise, Inc. for 55 fixed automated license plate recognition (ALPR) locations using Axon Outpost, six additional Axon Fleet 3 in-car video and mobile ALPR systems, and 120 Axon AI Assistant licenses for the Police Department, for a 49-month term beginning October 1, 2026, in an amount not to exceed \$661,687.54.

FISCAL IMPACT

Axon quote Q-908995-001, issued August 19, 2026, provides a 49-month term from October 1, 2026, through October 31, 2030. The quote lists a Total Contract Value of \$661,687.54, including estimated tax.

- FY 2026-27: \$175,403.86 (\$135,500.06 due September 1, 2026, and \$39,903.80 due June 1, 2027).
- FY 2027-28: \$135,500.04, due October 1, 2027.
- FY 2028-29: \$175,391.87, due October 1, 2028.
- FY 2029-30: \$175,391.77, due October 1, 2029.

Funding for FY 2026-27 has been identified within the existing Police Department General Fund budget; payments in future fiscal years will remain subject to the annual budget process.

DISCUSSION

Background and System Consolidation

ALPR and in-car video are established technologies at the Antioch Police Department (APD). The Department currently operates fixed ALPR cameras through Motorola and

Flock. Motorola is decommissioning its ALPR platform, and the proposed purchase would replace and consolidate the two fixed systems into a single Axon network while expanding fixed coverage. The updated quote stages 38 Axon Outpost locations beginning in 2026 and 17 additional locations in 2027, for 55 fixed ALPR locations under the agreement. The purchase also adds six Fleet 3 systems to support the Department's expanding patrol fleet and 120 Axon AI Assistant licenses.

APD already uses Axon Body 4 cameras, Axon Fleet in-car cameras, and Axon Evidence as its primary digital evidence environment. Officers, supervisors, investigators, prosecutors, and evidence personnel are familiar with the workflow. Consolidating the fixed ALPR network, added Fleet systems, and AI Assistant within that environment reduces separate accounts, evidence transfers, integrations, audit systems, training burdens, and vendor support relationships.

ALPR Public Safety Value and Evidence

ALPR helps officers and investigators identify vehicles associated with shootings, robberies, burglaries, stolen vehicles, hit-and-run collisions, organized theft, missing persons, illegal sideshows, and other serious incidents. Fixed cameras can alert officers when a vehicle on an authorized hotlist is detected, while authorized historical searches can help develop timelines and investigative leads. The six additional Fleet 3 systems will extend mobile ALPR capability to additional patrol vehicles. ALPR results are investigative leads and do not replace officer verification, lawful investigative steps, or independent judgment.

Bay Area agencies report measurable ALPR outcomes. Berkeley reported at least 37 stolen-vehicle recoveries, 58 arrests, and support in 121 cases in 2025. South San Francisco reported 108 stolen vehicles recovered and 40 related arrests from 2022 through 2024; stolen-vehicle incidents fell 19 percent during that period, a decline the City attributed in part to ALPR. Piedmont reported 33 arrests and 37 recovered vehicles in 2023, and San Francisco reported its ALPR system assisted in 207 arrests by April 2025. A 2025 peer-reviewed Atlantic City evaluation also found a major ALPR expansion was associated with reductions in shootings, motor-vehicle theft, and property crime. These results demonstrate investigative value but do not mean ALPR alone causes broader crime reductions.

ALPR Governance, Privacy, and Accountability

APD already has an ALPR policy in place; this procurement changes the technology platform and expands capacity, but it does not create a new authority to use ALPR. Policy 422 restricts ALPR use to official law enforcement business, prohibits unauthorized use, requires Department-approved training, and directs officers, when practicable, to verify an ALPR response through police computer databases before taking enforcement action based solely on an alert (Policy 422.4). The policy also requires safeguarded, login/password-protected access that documents the user, date, and time; limits access to legitimate law enforcement purposes; and calls for regular audits (Policy 422.6). Outside law enforcement requests must be in writing, identify the requesting agency and person, state the intended purpose, be approved before release,

and be retained on file (Policy 422.7). APD's current operating rules add a further requirement that historical searches be tied to a specific police case or CAD event and include a specific investigative reason. APD does not share or provide access to ALPR data with federal or out-of-state agencies in accordance with the California Values Act (SB 54).

These controls will carry forward to the Axon platform. Under Axon's governance model, the City retains control of its ALPR data, sharing is not automatic, and access is logged and auditable. APD will not provide direct or standing ALPR access to federal or out-of-state law enforcement agencies. Any authorized request from another California law enforcement agency must have a lawful investigative purpose and remain subject to APD approval, policy, logging, and audit. The system does not use facial recognition or make enforcement decisions.

In-Car Video Expansion

APD already uses Axon Fleet in-car cameras in patrol vehicles. The six Fleet 3 systems included in this agreement will be installed in additional patrol vehicles as the Department's fleet expands. They will extend in-car video and mobile ALPR coverage while keeping vehicle evidence within the same Axon Evidence environment used today for chain of custody, permissions, auditing, legal holds, and disclosure. No separate in-car video platform or evidence workflow is being introduced.

Axon AI Assistant and Language Access

Axon AI Assistant licenses adds an audible language translation feature to the Body 4 camera already worn by officers in the field. This provides language translation assistance in more than 50 languages, including Spanish, Tagalog, Vietnamese, Arabic, Mandarin Chinese, Hindi, and Persian, all within language groups identified in APD's Language Access Plan. The feature is manually activated and uses a push-to-talk workflow; it is not passively or continuously listening. When translation is activated, the interaction is recorded through the body-worn-camera system and use is auditable in Axon Evidence. This gives officers an immediate communication tool during traffic stops, calls for service, public-assistance contacts, and initial investigations and supports APD's obligations under the Department of Justice Memorandum of Agreement and the Department's Language Access Plan to provide timely and meaningful language access.

The Assistant supplements, rather than replaces, bilingual officers and qualified human interpreters. Personnel will receive training on appropriate use, limitations, verification, and supervisory oversight before deployment.

SOLE SOURCE JUSTIFICATION

Staff recommends sole source procurement to standardize on the Axon platform APD already uses for body-worn cameras, in-car video, and Evidence.com. One environment provides common accounts and permissions, familiar evidence handling and chain of custody, coordinated auditing, a common training framework, and single-vendor

support. Procuring separate fixed ALPR, in-car video, and field-assistant systems would recreate the fragmented accounts, integrations, evidence transfers, security reviews, training, and support relationships this project is intended to reduce. Other vendors sell standalone products, but the City's operational requirement is an integrated design compatible with Axon systems already deployed by APD.

Antioch Municipal Code section 3-4.12(B) permits sole source purchasing for unique, proprietary, or specific-design goods and services, including hardware, software, and communications equipment.

ATTACHMENTS

- A. Resolution
- B. Axon Quote Q-908995-001
- C. Axon Vehicle Intelligence Governance and Technology Materials
- D. Axon AI Assistant and Real-Time Translation Materials

RESOLUTION NO. 2026/XX

**RESOLUTION OF THE CITY COUNCIL OF THE CITY OF ANTIOCH AUTHORIZING
A SOLE SOURCE AGREEMENT WITH AXON ENTERPRISE, INC. FOR
AUTOMATED LICENSE PLATE RECOGNITION , IN-CAR VIDEO, AND
INTEGRATED PUBLIC SAFETY TECHNOLOGY SYSTEMS NOT TO EXCEED
\$661,687.54**

WHEREAS, the Police Department currently operates Motorola and Flock ALPR systems, and Motorola is decommissioning its platform, requiring replacement and consolidation of the City's fixed ALPR systems; and

WHEREAS, the Police Department already uses Axon Fleet in-car cameras, Axon Body 4 cameras, and Evidence platforms, and the proposed purchase includes 55 fixed Axon Outpost ALPR locations, staged as 38 beginning in 2026 and 17 additional locations in 2027, six additional Axon Fleet 3 in-car video and mobile ALPR systems for additional patrol vehicles as the Department's fleet expands, and 120 Axon AI Assistant licenses; and

WHEREAS, APD's existing Policy 422 governs ALPR use and restricts it to official law enforcement purposes, requires Department-approved training, safeguards and logs access, limits stored-data access to legitimate law enforcement purposes, calls for regular audits, does not share data with federal or out-of-state agencies, complies with the California Values Act (SB 54) and requires review and approval of outside law enforcement requests; and

WHEREAS, Axon AI Assistant provides real-time translation via the Body 4 camera currently used by officers in more than 50 languages, supporting field operations and APD's language-access responsibilities; and

WHEREAS, standardizing the replacement and expanded fixed ALPR network, additional Fleet systems, and AI Assistant within APD's existing Axon environment provides common training, evidence handling, permissions, auditing, and vendor support and supports sole source procurement under Antioch Municipal Code section 3-4.12(B);

NOW, THEREFORE, BE IT RESOLVED that the City Council hereby authorizes the Acting City Manager, or designee, to execute a sole source agreement with Axon Enterprise, Inc., in a form approved by the City Attorney, for the technology described above for a 49-month term not to exceed \$661,687.54.

* * * * *

I HEREBY CERTIFY that the foregoing resolution was passed and adopted by the City Council of the City of Antioch at a regular meeting thereof, held on the 25th day of August 2026, by the following vote:

AYES:

NOES:

ABSTAINED:

ABSENT:

MICHAEL J. MANDY
CITY CLERK OF THE CITY OF ANTIOCH



Axon Enterprise, Inc.

17800 N 85th St, Scottsdale, Arizona 85255, United States
VAT: 86-0741227
Domestic: (800) 978-2737 | International: +1 800.978.2737

ATTACHMENT B

Q-908995-001

Acct: 147404

Issued
Expires
Payment Terms
Mode of Delivery

Aug 19, 2026
Aug 31, 2026
N30
AUTO-GND

Antioch Police Department - CA

Currency: USD

CUSTOMER DETAILS

SHIP TO	BILL TO	SALES REPRESENTATIVE	PRIMARY CONTACT
Antioch Police Department - CA 300 L ST ANTIOCH, CA 94509-1159 USA	Antioch Police Department - CA 300 L ST ANTIOCH, CA 94509-1159 USA	Tierney Stuhr Phone: (480) 712-4910 Email: tstuhr@axon.com	William William Whitaker Phone: (925) 354-8981 Email: ww Whitaker@ci.antioch.ca.us

QUOTE SUMMARY

Program Length	49 Months
Contract Start	Oct 1, 2026
Contract End	Oct 31, 2030
TOTAL CONTRACT	
Net Total	\$645,529.50
Est. Tax	\$16,157.80
Total Contract Value	\$661,687.30

PAYMENT SUMMARY

DATE	SUBTOTAL	EST. TAX	TOTAL
Sep 1, 2026	\$132,453.38	\$3,046.68	\$135,500.06
Jun 1, 2027	\$38,579.80	\$1,324.00	\$39,903.80
Oct 1, 2027	\$132,453.36	\$3,046.68	\$135,500.04
Oct 1, 2028	\$171,021.60	\$4,370.27	\$175,391.87
Oct 1, 2029	\$171,021.60	\$4,370.17	\$175,391.77
Total	\$645,529.74	\$16,157.80	\$661,687.54



Axon Enterprise, Inc.

Doc ID: 36476a9332e2

Tax estimates are approximate and subject to change at time of invoicing.

SUMMARY PRICING FOR TERM

SUMMARY PRICING										
ITEM	DESCRIPTION	QTY	TERM	UN-BUNDLED	LIST PRICE	NET PRICE	SUBTOTAL	EST. TAX	TOTAL	
80462	True Up - Fleet 3 Advanced with TAP	6	9 (2/2030)	—	\$108.00	\$108.00	\$5,832.00	\$568.62	\$6,400.62	
103070	Outpost TAP Bundle True-Up	33	11 (10/2026)	—	\$100.83	\$73.56	\$26,701.29	\$2,603.39	\$29,304.68	
102182	Outpost Bundle True-Up	17	20 (3/2029)	—	\$68.49	\$0.00	\$0.00	\$0.00	\$0.00	
102011	Axon AI Assistant	120	49 (10/2026)	—	\$31.93	\$29.27	\$172,118.40	\$0.00	\$172,118.40	
F00011	Bundle - Fleet Cradlepoint R920 Single Modem Kit	6	49 (10/2026)	—	\$1,464.00	\$214.00	\$1,284.00	\$125.18	\$1,409.18	
Fleet3A	Fleet 3 Advanced	6	49 (10/2026)	\$304.95	\$304.95	\$221.96	\$65,256.24	\$1,937.01	\$67,193.25	
80402	Axon Fleet - Real-Time Location, Alerts & Livestream License	49	9 (2/2030)	—	\$15.00	\$0.00	\$0.00	\$0.00	\$0.00	
B00076	Outpost TAP Plan	33	49 (10/2026)	\$395.30	\$395.32	\$135.45	\$219,021.29	\$6,952.43	\$225,973.72	
102703	Axon Outpost - Warranty - Vandalism/Accident Extension	33	38 (9/2027)	—	\$1,200.00	\$1,200.00	\$39,600.00	\$0.00	\$39,600.00	
B00075	Outpost Plan	5	49 (10/2026)	\$322.81	\$322.80	\$0.00	\$0.00	\$0.00	\$0.00	
B00076	Outpost TAP Plan	17	40 (7/2027)	\$428.03	\$428.01	\$140.17	\$95,316.28	\$3,971.17	\$99,287.45	
102703	Axon Outpost - Warranty - Vandalism/Accident Extension	17	29 (6/2028)	—	\$1,200.00	\$1,200.00	\$20,400.00	\$0.00	\$20,400.00	
							SUBTOTAL	EST. TAX	TOTAL	
Total							\$645,529.50	\$16,157.80	\$661,687.30	

DELIVERY SCHEDULE

ESTIMATED SHIPPING DATE: Sep 1, 2026	
Shipping Location: 300 L ST, ANTIOCH, CA, 94509-1159, USA	
HARDWARE	QTY
Axon Fleet - Cradlepoint R920-C7A+5Yr Netcloud	6
Axon Fleet 3 - Standard 2 Camera Kit	6
Axon Outpost - Battery & Charger Enclosure - Extended	38
Axon Outpost - Camera	39
Axon Outpost - Pole - Standard	38
Axon Outpost - Solar Panel - 100W	38
Axon Outpost - Standard Solar Hardware Kit	38
Axon Outpost - Top Mount End Cap - Standard	38
Axon Signal Vehicle	6
SERVICES	QTY
Axon Fleet 3 - Deployment Per Vehicle - Not Oversized	6
Axon Fleet 3 - SIM Insertion - VZW 4FF	6
Axon Outpost - Standard Installation	38
Axon Outpost - Upgrade Installation	33
WARRANTIES	QTY
Axon Fleet 3 - Ext Warranty - 2 Camera Kit	6
Axon Outpost - Ext Warranty - Camera	39
Axon Outpost - Maintenance	38
Axon Outpost - Warranty - Vandalism/Accident Extension	33
Axon Signal - Ext Warranty - Signal Vehicle	6
ESTIMATED SHIPPING DATE: Oct 1, 2026	
Shipping Location: 300 L ST, ANTIOCH, CA, 94509-1159, USA	
SOFTWARE	QTY
Axon AI Assistant	120
Axon Evidence - Fleet Vehicle License	6
Axon Evidence - Storage - Fleet 1 Camera Unlimited	12
Axon Fleet - Real-Time Location, Alerts & Livestream License	6
Axon Fleet 3 - ALPR License - 1 Camera	6
Axon Vehicle Intelligence - ALPR License	38
ESTIMATED SHIPPING DATE: Jun 1, 2027	
Shipping Location: 300 L ST, ANTIOCH, CA, 94509-1159, USA	
HARDWARE	QTY
Axon Outpost - Battery & Charger Enclosure - Extended	17
Axon Outpost - Camera	17
Axon Outpost - Pole - Standard	17
Axon Outpost - Solar Panel - 100W	17
Axon Outpost - Standard Solar Hardware Kit	17



Axon Outpost - Top Mount End Cap - Standard	17
SERVICES	QTY
Axon Outpost - Standard Installation	17
Axon Outpost - Upgrade Installation	17
WARRANTIES	QTY
Axon Outpost - Ext Warranty - Camera	17
Axon Outpost - Maintenance	17
Axon Outpost - Warranty - Vandalism/Accident Extension	17
ESTIMATED SHIPPING DATE: Jul 1, 2027	
Shipping Location: 300 L ST, ANTIOCH, CA, 94509-1159, USA	
SOFTWARE	QTY
Axon Vehicle Intelligence - ALPR License	17
ESTIMATED SHIPPING DATE: Feb 1, 2030	
Shipping Location: 300 L ST, ANTIOCH, CA, 94509-1159, USA	
SOFTWARE	QTY
Axon Fleet - Real-Time Location, Alerts & Livestream License	49
ESTIMATED SHIPPING DATE: Oct 1, 2030	
Shipping Location: 300 L ST, ANTIOCH, CA, 94509-1159, USA	
HARDWARE	QTY
Axon Fleet - TAP Refresh 1 - 2 Camera Kit	6
Axon Outpost - TAP Refresh One - Battery Enclosure Extended	50
Axon Outpost - TAP Refresh One - Camera	51



TERMS & CONDITIONS

Tax is estimated based on rates applicable at date of quote and subject to change at time of invoicing. If a tax exemption certificate should be applied, please submit prior to invoicing.

STANDARD TERMS AND CONDITIONS

Axon Master Services and Purchasing Agreement:

This Quote is limited to and conditional upon your acceptance of the provisions set forth herein and Axon's Master Services and Purchasing Agreement (posted at <https://www.axon.com/sales-terms-and-conditions>), as well as the attached Statement of Work (SOW) for Axon Fleet and/or Axon Interview Room purchase, if applicable. In the event you and Axon have entered into a prior agreement to govern all future purchases, that agreement shall govern to the extent it includes the products and services being purchased and does not conflict with the Axon Customer Experience Improvement Program Appendix as described below.

Cradlepoint Terms and Conditions:

By accepting this Quote including Cradlepoint products, Customer designates and authorizes Axon as its partner of record for purposes of Cradlepoint product renewals, support coordination, and other relevant functions. This designation applies to all Cradlepoint products acquired by Customer during the Subscription Term of this Quote whether directly from Cradlepoint, through Axon, or through any third-party vendor or distributor. Axon shall have no liability to Customer or any third party arising out of or relating to Axon's acts or omissions as the partner of record. Customer has the right to opt out of this authorization at any time by providing prior written notification to both Axon and Cradlepoint. Upon such notification, the designation will be removed. This authorization remains effective until formally removed in accordance with this section or as otherwise agreed between the parties in the Agreement.

ACEIP:

The Axon Customer Experience Improvement Program Appendix, which includes the sharing of de-identified segments of Agency Content with Axon to develop new products and improve your product experience (posted at www.axon.com/legal/sales-terms-and-conditions), is incorporated herein by reference. By signing below, you agree to the terms of the Axon Customer Experience Improvement Program.

Acceptance of Terms:

Any purchase order issued in response to this Quote is subject solely to the above referenced terms and conditions. By signing below, you represent that you are lawfully able to enter into contracts. If you are signing on behalf of an entity (including but not limited to the company, municipality, or government agency for whom you work), you represent to Axon that you have legal authority to bind that entity. If you do not have this authority, please do not sign this Quote.

EXCEPTIONS TO STANDARD TERMS AND CONDITIONS

Rewrite Estimates

Estimated Amounts and Contract Terminations. Any amounts stated as due under existing or terminated contracts — including contract transfer balances carried forward to new or pending contracts — are estimates based on payments received as of the calculation date. These estimates may be adjusted if new contracts are not executed on the anticipated dates or if expected payments are not made.

Refresh Shipment Timing

Technology Assurance Plan (TAP) Refresh Prior to Renewal. For Customers with expiring agreements that include TAP refresh rights, Axon may, in its discretion, ship refresh hardware under the existing contract while renewal or replacement agreements are in progress. Any such shipments will be deemed made under the terms of the existing contract until the new contract is fully executed, after which any applicable updates, fees, or adjustments will apply.

Shipment Timing

Shipment Variance. Estimated shipment dates are provided for planning purposes only and are not guarantees. Axon may ship hardware before or after the estimated shipment date, and failure to meet an estimated shipment date will not, by itself, constitute a breach, provided Axon uses commercially reasonable efforts to meet estimated shipment dates.

OUTPOST SOW

1. Purpose

This Statement of Work ("SOW") outlines the scope, responsibilities, and installation details for Axon as part of the Customer's purchase of Axon Outpost. This SOW operates under the terms of the Agreement. All capitalized terms in this SOW shall have the same meaning as the Agreement.

2. Scope of Work

Axon and Axon authorized subcontractors will install and maintain Axon Outpost on selected Customer owned properties.

3. Installation Location

Customer grants Axon the right to install and maintain Axon Outpost at location sites approved by Axon.

3.1. If location sites have not been selected or assessed at the time of contract signature, Axon reserves the right to invoice the Customer for additional install complexities not accounted for in the initial quote.

4. Installation, Validation, and Support

4.1. Site Selection and Assessment. Axon will support site selection and assessment. Assessments may be conducted virtually or in-person and may include confirmation of visibility/coverage, cellular strength, solar feasibility, and access to AC power sources.

4.1.1. For all existing infrastructure installation sites, Customer is responsible for condition of existing infrastructure.

4.1.2. If during a site walk it has been deemed that an installation is more complex than initially quoted, Axon reserves the right to invoice Customer for the additional cost of installation.

4.1.3. If Axon deems a selected location site is not suitable for installation, a new site must be selected and assessed.

4.2. Permitting. Axon will assist with obtaining the necessary local, state, or Federal approvals before installing Outpost. All permitting fees are the responsibility of the customer. All permit licenses will be in the name of the customer.

4.3. Installation. Axon will install all Axon Outpost hardware and agreed-upon pole (where applicable).

4.3.1. Solar Sites. For sites with solar power, Axon will: (a) install the Outpost camera, battery, and solar panel; (b) ensure the camera is connected to power and LTE; (c) ensure the camera is set at the optimal capture angle; (d) ensure the panel is installed for optimal sun exposure.

4.3.2. AC Sites. For sites with AC power, Axon will: (a) install the Outpost camera and AC adapter; (b) ensure the camera is set at the optimal capture angle. Axon will not conduct any electrical work to connect the AC adapter to power. The customer may work with a licensed electrician to connect the camera to power. Or, if requested, the customer may request for Axon to coordinate with a licensed electrician for an additional cost.



4.3.3. Existing Infrastructure Installations. If selected infrastructure has existing camera(s), Axon will remove the hardware before installing Outpost. Axon will not dispose of equipment, repair any surfaces or structures, or remove underground cables or conduit.

4.3.4. Standard and Advanced Installations. For Standard or Advanced installations, Axon will install a breakaway or MASH approved pole, respectively. Axon will call 811 prior to installation.

4.3.5. DOT Pole Installation Service. Axon will install Outpost on existing DOT poles and ensure compliance with DOT guidelines. Axon will not install DOT poles.

4.3.6. Complex Location Sites. Complex location sites require a custom SOW and include, but are not limited to, toll booths, bridges and overpasses, federal or military land, areas with restricted access or high security, flood zones, railway crossing, mountainous or hilly terrain.

4.3.7. Exclusions. Installation services do not include the following, unless specifically scoped in a custom SOW: electrical work, concrete drilling, bucket truck or non-standard equipment rental, trenching, tree trimming, custom engineered drawings or traffic plans, traffic control beyond basic MUTCD traffic control, environmental impact studies.

5. Power Requirements

5.1. AC-Powered Sites. Axon will provide all necessary equipment compatible with standard AC power configurations. Customer is responsible for contracting a licensed electrician to ensure installation meets NEC (National Electrical Code) standards and the power must be continuous and non-switched to support uninterrupted system operation; all electrical work must comply with local codes and safety regulations.

5.2. Solar-Powered Sites. Installation sites must offer unobstructed southern exposure to maximize solar efficiency. Axon will assess solar viability during site assessment, including shading, positioning, and mounting considerations. Customer will ensure the selected location sites must maintain direct, unobstructed visibility to the sky to ensure consistent solar energy capture. Customer agrees to help maintain environmental conditions that support reliable solar performance (e.g., minimizing nearby shade, vegetation growth).

6. Traffic Control

Axon will provide basic MUTCD traffic control and provide necessary traffic signs, cones, and temporary barriers.

7. Dependencies and Potential Delays

Installation is subject to but not limited by the following factors, which may affect scheduling and completion: delays due to local permitting requirements or jurisdictional approvals; availability and completion of necessary electrical work at the installation site (for AC-powered setups); coordination with Customer and subcontractors, including restricted hours or special access requirements; weather-related delays that may impact site safety or installation feasibility; or any site-specific safety protocols or regulatory requirements that must be satisfied prior to deployment.

8. Training and Onboarding

Axon's team will provide hands-on training for relevant personnel, user credentials and access to supporting applications, and operational guidance tailored to the current system configuration.

9. General Responsibilities

9.1. Axon will: (a) install, configure, and maintain all hardware at designated location site; (b) validate system power, connectivity, and functionality of Outpost; (c) integrate Outpost with Fusus, including NCIC and state hotlists; and (d) will provide training, documentation, and technical support to Customer personnel.

9.2. Customer will: (a) fund and maintain all legally required permits, authorizations, and/or licensing to place, maintain, and/or remove the Outpost at the installation sites; (b) ensure access to installation sites, support device placement communication, and coordinate internally (e.g., facilities, IT, legal, public safety) to facilitate deployment; (c) support scheduling for permitting and local compliance requirements; (d) designate a primary and backup point of contact; and (e) support site selection, utility clearance, and installation approvals.

Signature

8/19/2026

Date Signed



Vehicle Intelligence

Built for Public Safety. Governed for Accountability.

Privacy, security, and compliance across Axon Vehicle Intelligence.

Agencies own and control their ALPR data. Sharing is explicit, permission-based, and revocable. Lawful requests go through the agency for read and hit data, not Axon. Retention is short, configurable, and automatically enforced. Every action is logged in immutable audit logs that hold up in a council chamber, a courtroom, or an oversight review.

That is the foundation Fleet 3, Outpost, and Lightpost are validated by independent third-party assessments, and proven across years of mobile ALPR deployments. The pages that follow show how it works in practice.

At a glance

Data ownership

Agencies own and control their ALPR data. Axon does not pool, resell, or independently disclose it.

Sharing

Off by default. Invite-only, visible, time-bound, and revocable.

Lawful requests

Routed to the agency as the data owner. Axon does not independently disclose customer data.

Federal access

No back door, no centralized pool. No automatic or standing federal access.

Retention

Agency-configured and automatically enforced. Non-evidentiary ALPR data purge per policy.

Audit

Every access logged with user, action, time, and stated reason, in immutable audit logs.

1. Your data, your control

Agencies own and control their ALPR data. Axon does not pool, resell, or independently disclose agency data. The eight points below are how that principle is implemented in practice.

Data ownership

The agency owns and controls its ALPR data. Axon does not have access to agency data and does not use agency data for any other purpose, including resale or independent analysis. Any external request for data, including subpoenas, warrants, or FOIA requests, would be directed to the agency itself, and the agency would determine how to respond under applicable law and its own policies.

Cross-agency sharing

Cross-agency sharing capabilities are planned for Q3 2026. Sharing relationships will be invite-only, visible, and revocable. Every relationship will be managed in the agency's Axon environment and will require an explicit invitation. Shared access will not create copies of records, recipient agencies will not take ownership, and there will be no national lookup or unrestricted network.

Lawful requests

Legal process requests are directed to the agency, and every step is logged. If a subpoena, warrant, or FOIA request is directed to Axon, we object and route it to the agency as the data owner. Axon Evidence audit logs preserve each step so councils and oversight bodies can confirm lawful procedures were followed.

Retention

Agencies set retention, and data is purged automatically. ALPR data is transferred into the agency's secure instance of Axon Evidence, where retention periods are configured. Non-evidentiary ALPR data is automatically deleted per agency policy. Axon provides recommended defaults, and agencies configure and control the settings themselves.

Access tracking

Every access is recorded, including who accessed the data, what actions were taken, and when access occurred. Immutable audit logs in Axon Evidence capture the user, action, time, and, when configured, the stated reason for access. Both Axon Evidence and Fusus provide audit capabilities that allow agencies to review activity at any time.

Sharing controls

Sharing is off by default, configurable based on agency policy, revocable, and can be time-bound. Sharing does not involve copying or redistributing ALPR data. Access is federated, allowing recipient agencies to query authorized data without taking ownership, and access can be revoked immediately by the donor agency.

AI model training

Axon may use transformed ALPR data from customers who have opted to participate in Axon's Customer Experience Improvement Program (ACEIP). Full plate reads are not used. Customers may opt out at any time by contacting aceip@axon.com.

Federal access

There is no back door or centralized pool for federal access. Any federal access requires either valid legal process directed to the agency or an agency-approved sharing relationship. Even when a sharing relationship exists, the agency must approve the request before data is shared. All access is permissioned and logged.

Transparency

Agencies receive access to the ALPR Policy and Usage Transparency Portal in Axon Evidence, which can be configured to publish retention policies, usage metrics, and program details on a public-facing website. Agencies control what is published and may disable the portal at any time.

2. Built to be secure

Axon ALPR cameras are engineered as field-deployable platforms with built-in protections aligned to Axon's Secure by Design principles, validated by internal testing and independent third-party assessments.

Device security and hardware integrity

- **Secure boot:** Each stage of the boot process is cryptographically validated; only Axon-signed firmware runs on the device.
- **Encrypted storage:** AES-256 encrypted partition with hardware-backed key protection covers ALPR reads, context video, authentication tokens, configuration files, and logs.
- **Physical security:** Physical interfaces (e.g., USB) support only approved functions and are locked against interactive access.
- **Controlled firmware and updates:** OTA firmware packages are cryptographically signed and validated before installation. Third-party penetration testing is performed under Axon's Trust & Assurance program.

Secure access and role management

- **Device access:** Devices have no exposed local login interface; configuration occurs through authenticated Axon workflows. Pairing requires authenticated provisioning via Axon's installer with signed tokens and encrypted channels.
- **Agency access controls:** Through Axon Evidence and Fusus, agencies assign to the device role-based permissions, enforce least-privilege access (including export and retention restrictions), and use SSO and MFA to align with their authentication standards.
- **Audit and accountability:** Every action, user activity, access attempts, configuration changes, sharing decisions, data exports, is recorded in immutable audit logs to maintain evidentiary integrity.

Data and network security

- **Data in transit:** TLS 1.2+ with cryptographic modules protects uploads to Axon Evidence and Fusus. Devices authenticate using hardware-protected certificates and signed tokens, preventing spoofing.
- **Data at rest:** AES-256 encryption protects all stored data.
- **Network defenses:** Firewall enforcement permits only essential outbound communication; inbound interfaces are restricted by default. Store-and-forward reliability buffers ALPR data on encrypted storage if connectivity is lost.

ALPR audit capability:

Beginning April 2026, agencies have access to a one-button ALPR audit report built directly into Axon Fusus.

The report is designed to make compliance reporting easy, repeatable, and defensible. It captures officer-level access activity including user identity, the action taken, timestamp, and the stated reason for each ALPR access. It'll also show activity by external agencies with whom you decide to share your ALPR data, when ALPR Sharing launches in Q3 2026.

The report is built for supervisory review, internal affairs, and oversight bodies that require full accountability detail. For external sharing such as FOIA requests, agencies can choose to remove PII and investigative details like officer name, plate number, and case number etc. before sharing the report. This pulls the data from the same immutable audit log infrastructure that underlies all of Axon Evidence.

3. Where Axon stands apart

The most important distinction is not the camera, it is how the system is structured after data is captured. Architecture determines exposure boundaries; configuration determines governance posture.

Design area	Agency-controlled model (Axon)	Shared / network-based model
Where data lives	Within an agency-controlled environment.	May be stored or accessed through shared or network-accessible environments.
Who can see data	Visibility unchanged unless the agency takes explicit action.	Visibility may expand based on participation, configuration, or system features.
How data is shared	Explicit, relationship-based sharing defined by the agency.	May be enabled through participation or system features.
Federal access	No back door or centralized pool for federal access. Any federal access requires a valid legal process directed to the agency or an agency-approved sharing relationship, and the agency must approve each request before data is shared.	Network-based architectures may create centralized data pools where legal process can be directed to the vendor rather than solely to the originating agency. Federal access pathways have been a documented focus of public scrutiny in this category.
Who can access	Limited to direct, authorized relationships.	May include indirect pathways such as partner agencies or shared query layers.
Retention	System-enforced based on agency policy.	Policy-defined with variable enforcement; exported data may persist outside controls.
Disclosure control	Agency retains full control.	May involve multiple entities.
Access tracking	Agency can directly review and explain all access.	Visibility into access may depend on system structure.
If something goes wrong	Issues typically contained to a single agency environment.	Impact scope may extend beyond one agency.
Independent validation	SOC 2 Type II, ISO 27001, ISO 27701, FedRAMP High, CJIS, see trust.axon.com .	Varies by vendor.

Agencies have used Fleet for years to deploy mobile ALPR responsibly, and that same foundation carries forward across fixed and mobile ALPR, sharing remains explicit, revocable, and fully auditable, whether the camera is in a patrol vehicle, on a roadside pole, or integrated into streetlight infrastructure. Adding fixed ALPR to an existing Fleet 3 deployment does not introduce a separate governance model: ALPR data flow into the same agency-controlled environment under the same retention, access, sharing, and audit controls.

Answers to the questions headlines are raising

Some of the most-asked questions in council chambers today come from headlines about other vendors in this category. Here is how Axon Vehicle Intelligence is structured to answer those questions directly.

Does Axon maintain a national pool of ALPR data?

No. ALPR data stays within the agency's environment unless the agency chooses to share it. There is no automatic cross-agency access, and the system does not connect to a national database. When an agency does choose to share, that access is limited, visible, and can be changed or revoked at any time. Nothing is shared by default, and agencies can only share data they own.

Can federal agencies automatically access our ALPR data?

No. The platform does not provide automatic or built-in access to any federal agency. There are no built-in pathways that route data outside the agency's controlled environment. Any request from a federal entity, like any other external request, would be directed to the agency itself, and the agency would determine how to respond based on its own policies and applicable law. Federal agencies do not receive automatic or standing access.

Can Axon disclose our agency's data without our permission?

No. The agency owns and controls its ALPR data. Axon does not have routine access to agency ALPR data and does not independently disclose it to any outside party. Subpoenas, warrants, and FOIA requests are routed to the agency as the data owner, and the agency determines how to respond based on its own policies and applicable law. All activity is logged so councils and oversight bodies can confirm lawful procedures were followed.

Is governance enforced by design or just by policy?

By design. Agency ownership, explicit sharing, enforceable retention, and immutable audit logs are built into the platform from the ground up, not added on top after the fact.

Can we use our own hotlists?

Axon supports both NCIC and agency-owned hotlists in a single platform. Axon pulls the NCIC hotlist on a daily cycle. Agencies can upload and manage their own hotlists directly in Evidence.com, with updates propagating to devices in minutes, giving agencies real-time control without depending on external update cycles. All hotlist data is encrypted in transit.

What this means in a council conversation

When an agency walks into a hearing on ALPR, the questions that decide the room are predictable: Where does our data live? Who can see it? Can it be shared without our permission? How long is it kept? Can a federal entity access it? Who is accountable when something goes wrong? Axon Vehicle Intelligence is structured so each of those questions has a clear, specific, system-enforced answer, not a policy promise layered over an architecture that allows otherwise.

Resources

Vehicle Intelligence overview: axon.com/products/vehicle-intelligence.

Trust, security certifications, and supporting documentation: trust.axon.com.

Axon Customer Experience Improvement Program: axon.com/aceip.

Axon cloud Services Policy: axon.com/legal/cloud-services-privacy-policy.

Responsible Innovation framework: axon.com/responsibility/responsible-innovation.



Council and Community Q&A

This Q&A answers common questions about automated license plate recognition (ALPR) programs and the Axon Vehicle Intelligence capabilities that support them. It explains system capabilities, governance controls and accountability in clear, practical terms.

System Overview

How is this different from another ALPR system?

The difference is in how the data is governed after capture. Axon Vehicle Intelligence is built around agency-controlled data: sharing is explicit and invite-only, no data is copied during sharing, recipient agencies cannot re-share data they receive, and all access and sharing activity is logged and reviewable by the owning agency. Each agency's data stays under its own control throughout the program's operation.

What It Is & What It Captures

What problem does this technology address?

Vehicle-related crime is a factor in many serious incidents, including stolen vehicles, hit-and-runs, missing persons cases and investigations that cross jurisdictions. In those situations, identifying a vehicle quickly can reduce the time it takes to locate a vehicle of interest and move an investigation forward. The system helps agencies confirm where a vehicle was seen and respond with better information, within defined limits on how data is collected, used and governed.

What data does the system collect?

The system captures a license plate image, a vehicle context image, basic vehicle attributes visible in the image such as color, make and vehicle type, and the time and location of the detection. The context image provides vehicle context for review. Because it is an image from the scene, it may incidentally include surroundings, signage or people in view. It is not analyzed for facial recognition or behavioral profiling. The system does not perform live registered-owner lookups or build a profile of a registered owner.

WHAT IT IS & WHAT IT CAPTURES – CONTINUED

Is this a form of surveillance?

ALPR cameras record vehicle detections at specific camera locations. The system does not use facial recognition, perform live registered-owner lookups or maintain continuous monitoring of individuals. The agency defines who can access the data, how long it is retained and what uses are authorized. Every search is tied to a named user and logged for review.

How does the agency decide where to deploy cameras?

Camera placement is an agency decision governed by the agency's operational needs, its policies and applicable law. Agencies should be prepared to explain the reasoning behind their deployment plan if asked in a public setting.

Tracking & Movement

Does this system track people?

No. The system captures vehicle detection information, not driver identity. License plate images and vehicle context are recorded at specific camera locations. It does not use facial recognition, perform live registered-owner lookups or maintain a live location feed on any person.

Could this be used to track where people go over time?

The system does not monitor people or maintain a live location feed on anyone. When investigating a specific vehicle, an authorized user can review where and when that plate was previously captured, within the agency's retention period. That search is tied to a named user and logged with the action, time and, where configured, stated reason. It is an investigative search of a known vehicle, bounded by retention and oversight, not continuous monitoring of the public.

Ownership, Sharing & Hotlists

Who owns and controls the data?

The agency owns and controls its ALPR data. Axon does not pool it, resell it, or disclose it except where legally required. Ownership does not change when data is preserved in Axon Evidence, and it does not change when an agency enables sharing. The agency decides retention, access and sharing. The system applies the configured controls. The agency remains responsible for policy, training and oversight.

Is this connected to a national database?

No. Data stays within the agency's environment unless the agency chooses to share it. There is no automatic cross-agency access, and the system does not place agency ALPR data into a national or pooled database. Visibility does not expand unless the agency takes deliberate action.

Can other agencies access the data?

Sharing is off by default and requires the owning agency's deliberate approval. Another agency can access data only through a specific sharing relationship approved by the owning agency. That access is invite-only, visible and revocable. Sharing does not copy agency ALPR data into a shared repository, transfer ownership or connect agency ALPR data to a national pool.

Can an agency that receives shared data re-share it with other agencies?

No. Re-sharing is architecturally impossible, not just prohibited by policy. Sharing is federated: no data is copied when a sharing relationship is established. Because no copy exists, a recipient agency never acquires ownership of shared data and cannot share it further. Agencies can only share ALPR data they own.

Can the agency audit how shared data is accessed?

Yes. When sharing is enabled, access to shared ALPR data is logged and reviewable by the owning agency. The audit record includes recipient activity against shared data and changes to sharing relationships over time, so the agency can review who had access during a specific period.

Can the agency control what ALPR searches are permitted?

Yes. The agency configures which offense categories are authorized for ALPR searches. That configuration applies system-wide, covering the agency's own users and any agencies the data is shared with, so a single standard governs how ALPR can be used across the program. When performing an ALPR search, users must enter an offense category. If that category is not on the agency's authorized list, the search does not return ALPR data.

OWNERSHIP, SHARING & HOTLISTS – CONTINUED

Can an agency use hotlists?

Yes. The agency controls which hotlists the system uses, including agency-owned lists, the National Crime Information Center (NCIC) and other official vehicle-status lists the agency is authorized to use. Any vehicle-status or owner-related details associated with a match come from the agency-authorized hotlist entry, not from a live registered-owner lookup.

Can the system look up who owns a vehicle?

No, not through a live registered-owner lookup. When a plate is read, the system compares it against agency-approved hotlists, which may include official vehicle-status lists the agency is legally authorized to use where configured. Any vehicle-status or owner-related details associated with a match come from the agency-authorized hotlist entry, not from a live registered-owner lookup.

Federal Access & Lawful Requests

Can federal agencies access the data?

There is no automatic, standing or built-in federal access to agency ALPR data through Axon. Because the agency owns and controls the data, a lawful request goes to the agency and its counsel to handle. If Axon receives such a request, Axon directs it to the agency as the data owner and discloses data only where legally required to do so.

What stops this from being used for immigration enforcement?

This is a local policy decision that the agency governs through its own policy and applicable law. The system provides no automatic, standing or built-in access to any federal agency, including immigration enforcement. If Axon receives a request for agency ALPR data, Axon directs it to the agency as the data owner and provides data only where legally required to do so. If a request goes directly to the agency, the agency decides how to respond under its own policy and applicable law.

Are ALPR records subject to public records requests?

Public records obligations depend on state and local law. The agency is responsible for reviewing and responding to public records requests under its policies and applicable law. ALPR reads, hits, audit records or related materials may require legal review and redaction before any external disclosure.

Retention, Oversight & Misuse

How long is data kept?

ALPR detection data is retained according to the agency's configured retention policy and removed when the applicable retention period expires. Detections preserved as evidence follow the agency's evidence retention rules. The agency sets retention periods according to its policy and applicable law, and the system enforces configured retention settings.

Is governance enforced by design or just by policy?

Policy sets the agency's rules. System design and configuration controls help enforce those rules, and audit records help the agency review use against them. Agency ownership, explicit sharing, configured retention and logged activity are reflected in how the system works and in the records the agency can review.

What prevents misuse of the system?

Access is limited to authorized users, and every ALPR search and relevant system action is logged with user, action, time and, where configured, stated reason. The agency can assign an audit owner, review activity on a defined cadence and enforce policy through investigation, access restrictions and disciplinary action when needed.

What happens if a hotlist match turns out to be incorrect?

A hotlist match generates an alert, not a stop. Officers review every alert and make all enforcement decisions based on their own assessment and applicable law. The system's role ends at detection. What happens next is governed by the agency's policies, officer training and applicable legal standards. The agency remains responsible for establishing how officers respond to alerts and how those decisions are reviewed over time.

Can an agency show the community how the system is governed?

Yes. Axon offers a public transparency portal an agency can use to disclose its data retention policies and available aggregate ALPR program information. The agency decides whether to publish it and controls which available elements appear. It stays off until the agency turns it on, and the agency can deactivate it at any time. It publishes aggregate information only, no plate numbers, images, individual records or camera locations. When an agency has sharing enabled, the portal can also disclose the partner agencies with whom data is shared.

RETENTION, OVERSIGHT & MISUSE – CONTINUED

How can the agency communicate program outcomes to the public over time?

The agency decides what to report, how often and through what channels. That may include aggregate metrics or approved examples such as recovered vehicles, investigative leads, missing person responses or AMBER and Silver Alert support, where available and appropriate. The Axon transparency portal gives agencies a tool to publish aggregate program information publicly. Agencies can also include outcome summaries in council presentations, annual reports or community updates. Agencies should not publish raw ALPR reads, plate numbers, images, exact camera locations, active investigation details, user-level audit logs or personal information.

AI & Scope

Does the system use AI to predict crime or flag people?

No. AI reads plate characters and basic vehicle attributes from images. It is not used to predict behavior, assign risk scores or identify individuals.

Is agency data used to train AI?

Axon's agreements with AI providers prohibit them from using agency data to train their models. Axon trains its own AI primarily on self-collected and synthetic data. An agency's ALPR data can also contribute to improving Axon's products, including AI, through the Axon Customer Experience Improvement Program (ACEIP). Participation is optional, and the agency can decline or withdraw at any time. Every approved ACEIP use case is published on Axon's [ACEIP transparency portal](#), with the data used and the safeguards applied listed for each.

What stops this from expanding into something more invasive over time?

New capabilities do not become part of the agency's program unless the agency approves or configures them under its policy and contract.

Vendor Access, Verification & Accuracy

Does Axon access agency data?

Axon has no standing access to agency ALPR data. Access occurs only when an agency initiates a specific support request. When that happens, access is temporary, limited to the stated purpose, logged and auditable by the agency.

Is the system independently verified?

Yes. Axon publishes current security and compliance documentation through trust.axon.com. Agencies should use that documentation to confirm which products, services and controls are in scope for each audit or certification. For governance detail, see the Axon Vehicle Intelligence Governance Guide.

What happens if the system gets it wrong?

Accuracy can vary with conditions such as lighting, camera angle and plate visibility. That is why a person reviews every alert before any action is taken. The agency has verification procedures to confirm information before an operational decision is made.

Cameras, Livestreaming & Recording

Do these cameras livestream and record, and how is that governed?

Livestreaming is permission-based and configurable. It is active only when an authorized user pulls up a feed for real-time viewing during an active situation. An agency controls whether it is enabled.

Video is handled under its own access, storage and retention controls, which are separate from how ALPR detection data is governed. Where an agency enables and configures recording, video is retained under the agency's video retention settings, not its ALPR retention settings. Video access is logged and auditable by the agency.

Core boundaries are built into how the system works. The system does not place agency ALPR data into a national pool, does not share data automatically, does not use facial recognition, does not perform live registered-owner lookups and does not automate enforcement. Within those boundaries, each agency configures retention, access, sharing, transparency and livestreaming or recording settings under its policy and applicable law.

For governance detail, see the Axon Vehicle Intelligence Governance Guide. For current security and certification documentation, see trust.axon.com.

Safer Streets, Data You Control

How intelligent technology is helping communities without asking them to give up control of their own data

A car is reported stolen at 7:40 on a Tuesday morning. By 8:15, it's found three miles away, parked outside an apartment complex, before the owner has even finished filling out the police report. A child goes missing from a park, and within the hour, a patrol officer gets an alert that the suspect vehicle just passed a nearby intersection. A hit-and-run leaves a family without answers, until a single camera on a streetlight two blocks away turns out to hold the one piece of information that closes the case.

This is what modern, AI-powered license plate recognition looks like in practice — not a surveillance dragnet, but a quiet, fast way of connecting a dot that used to take days, or never got connected at all. For the communities using it responsibly, it's become one of the more effective tools for solving the crimes that actually keep people up at night: stolen vehicles, missing persons, hit-and-runs, and the kind of organized theft rings that move fast across city lines.

But a tool this capable also deserves real scrutiny — and it should have to earn a community's trust, not just ask for it. That's where the conversation usually turns, and where it should turn. Who owns this data? Who can see it? Can it end up somewhere the community never agreed to? How long does it stick around? And if something ever goes wrong, is there an honest paper trail, or just a promise?

Your Community's Data Stays Your Community's Data

With Axon Vehicle Intelligence, the agency owns its license plate data. Axon doesn't pool it, doesn't resell it, and doesn't use it for anything beyond what the agency itself directs. There's no hidden national database quietly aggregating every community's plate reads into one place. If your community never chooses to share its data, it simply doesn't leave your community.

Sharing Only Happens When Your Community Says So

Nothing is shared by default. If an agency wants to collaborate with a neighboring department — which can genuinely help solve cross-jurisdiction crime — that relationship has to be explicitly invited, it's fully visible to the agency the whole time, and it can be revoked instantly if the community's priorities or leadership change. No open network. No standing access. No exceptions quietly baked into the fine print.

No Back Door for Federal Access

This is often the first question raised in a council chamber, and it deserves a direct answer: there is no automatic or standing federal access to a community's license plate data, and no centralized pool a federal agency can simply query. Any request — federal, state, or otherwise — has to go through the agency itself, following that agency's own policies and the law. Your community's elected leadership and police department stay the ones answering that question, not a vendor answering it for them behind closed doors.

Data Doesn't Sit Around Forever

Retention is set by the agency, not by Axon, and once that window closes, non-evidentiary data is deleted automatically — no one has to remember to do it, and no one can quietly decide to keep it longer. A community that wants a short retention window gets a short retention window, enforced by the system itself, not by a policy document that only works if everyone remembers to follow it.

Every Use Leaves a Record That Holds Up

Every time the system is accessed — who looked, what they did, when, and why — it's captured in an audit log that can't be edited after the fact. That's what makes it possible to answer tough questions honestly in a council meeting, in a courtroom, or in front of an oversight board: not a promise that things were done right, but a record that shows it.

Independently Verified Security

None of this is just Axon's word to take. The security this is built on — encryption, access controls, breach protections — has been independently verified against some of the most rigorous standards that exist: SOC 2 Type II, ISO 27001, ISO 27701, FedRAMP High, and CJIS. Those aren't marketing terms; they're independent audits that have to be earned and re-earned, not claimed once and forgotten.

Safety and Accountability, Together

The honest version of this conversation isn't "trust us." It's this: a community can have a genuinely powerful tool for solving real crimes — recovering stolen cars, finding missing kids, closing hit-and-runs — without handing over control of its own data to do it. The technology is built so the hard questions have real, specific, verifiable answers, not vague reassurances layered on top of a system that could just as easily work the other way.

That's the balance this is designed around: safer streets, and a community that never has to wonder who's really in control of the tool making them safer.

Real-Time Translation — Axon Body 4

Frequently Asked Questions for City Council

This one-pager anticipates the questions Council members are most likely to raise about the Real-Time Translation feature available on Axon Body 4 cameras, covering how it works, its limitations, evidentiary use, data security, and oversight.

Feature Overview

What exactly does this feature do?

It lets an officer hold a two-way voice conversation with someone who speaks a different language, translated in real time through the body-worn camera. No app, no phone, no separate device — it's built into the Axon Body 4.

How is it activated — is it always listening?

No. It only activates when an officer manually double-presses a programmable button, and only captures audio while a second button is held down (push-to-talk). There is no passive or continuous listening.

How many languages, and how good is the translation?

50+ languages with strong reliability for understanding “main intent” (Spanish, Mandarin, Vietnamese, Tagalog, Arabic, Russian, and others are all covered). It is not positioned as certified-interpreter-quality — it is built for quick, everyday encounters, not high-stakes or evidentiary situations.

Appropriate Use & Human Interpreters

When is it appropriate to use, and when isn't it?

Designed for routine, lower-stakes interactions — traffic stops, minor incident reports, public event assistance. For witness statements, high-stakes incidents, or anything requiring certified accuracy, officers are still directed to use human interpreters (certified bilingual officers, LanguageLine, etc.).

Does this replace bilingual officers or human interpreters?

No. Certified human translators remain necessary for complex or high-stakes situations, and bilingual officers continue to be relied on for those cases.

Could this raise union or staffing concerns for bilingual officers?

The tool is designed to support officers who don't speak a second language and reduce staffing strain — it is not meant to replace bilingual officers, who are still needed for complex, high-stakes, and evidentiary interactions.

Recording & Evidentiary Use

Is every interaction recorded?

Yes. Activating translation also starts audio/video recording, uploaded to Evidence.com like all other body-camera footage — the same retention and chain-of-custody rules the department already uses.

Can this translated audio be used as evidence in court?

Not reliably on its own — AI-generated translations may not meet formal evidentiary admissibility standards in most jurisdictions. The underlying recording, verified separately by a human translator, is what would support case documentation.

Oversight, Accuracy & Transparency

What oversight and accountability exists for how it's used?

Every use is logged in the device's audit trail on Evidence.com, and supervisors can review who used translation, when, and for how long, per the agency's own access permissions.

What happens if the tool mis-identifies the language or mistranslates?

The officer can reset and manually specify the correct language. If detection still fails or the tool clearly isn't working, the guidance is to fall back to a human translator.

Are community members told they're being translated or recorded?

Officers are trained to state plainly that they are using the camera to translate the conversation — a suggested standard preamble is provided in training — though exact wording is left to officer judgment based on the situation.

Data, Cost & Certification

What data is retained, and is it secure?

No separate transcripts or audio are stored beyond what's already captured in normal body-camera evidence retention; usage metadata (device ID, timestamps) is retained for one year in Axon's secure logging systems. No data is shared with third-party AI model providers — everything stays within Axon's secure cloud.

Is there a cost impact?

No separate data usage charge — it's included in the Camera Connectivity Pack, which is required to use the feature (i.e., the agency needs Axon Respond, Respond+, or the Device Connectivity Pack already in place).

Is it certified for government or public-sector use?

Yes — certified at the FedRAMP Moderate level.

What if a camera is lost or stolen?

It can be immediately marked lost in Evidence.com, which disables the device's access to the feature.

Source: Axon Real-Time Translation product documentation and Axon Assistant PRFAQ.