

INTERGOVERNMENTAL AGREEMENT

Agency-Procured Automated License Plate Reader Deployment on State Right-of-Way and DPS Data Governance

This Intergovernmental Agreement (“Agreement”) is entered into by and between the Arizona Department of Public Safety (“DPS”) and _____ (“Agency”). DPS and Agency are each a “Party” and collectively the “Parties.”

1. Authority and Purpose

This Agreement is entered into pursuant to A.R.S. § 11-952 and any other applicable authority of the Parties.

The purpose of this Agreement is to establish the terms under which Agency may directly procure, pay for, install, maintain, and operate an automated license plate reader system (“ALPR” or “LPR”) on or near Arizona state highway or interstate highway right-of-way, subject to DPS review, DPS operational approval, DPS data-governance requirements, ADOT permitting requirements, and the use and sharing limitations in this Agreement.

The Parties intend that the Agency, not DPS, will be responsible for procurement, vendor contracting, payment, installation costs and coordination with ADOT, subscription costs, maintenance costs, repair costs, replacement costs, utility costs, and removal costs unless the Parties expressly agree otherwise in writing. DPS will not serve as a pass-through funding entity for Agency’s procurement or vendor payments.

DPS approval is conditioned on Agency’s continued compliance with this Agreement, DPS policy and operational direction, applicable law, Agency’s acquisition and maintenance of an ADOT encroachment permit, and all DPS-approved data access, sharing, retention, audit, and security requirements.

Nothing in this Agreement replaces any required ADOT permit, right-of-way approval, utility approval, procurement approval, funding approval, cybersecurity approval, or other required authorization. Nothing in this Agreement may limit the ADOT Director’s jurisdiction or control over the highway per A.R.S § 28-363(A)(5).

2. Definitions

“Administration of Criminal Justice” means the performance of criminal justice activities, including detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders, as well as criminal identification activities and the collection, storage, and dissemination of criminal history record information. For this Agreement, this definition is used as an access and use limitation consistent with CJIS/ACJIS use criteria and does not convert ALPR data into criminal history record information unless otherwise required by law.

“ALPR Data” means license-plate images, plate-read data, time/date/location information, vehicle images, metadata, alert information, search results, audit logs, exports, hot-list hits,

vendor reports, and any record or information generated, stored, queried, received, or disclosed through the ALPR system.

“Approved Participating Agency” means a public agency that has executed a DPS-approved ALPR agreement or system MOU, completed DPS-required access requirements and ensured that its authorized users hold and maintain current ACJIS Terminal Operator Certification, and, where applicable, obtained, or agrees to obtain, and maintain an ADOT encroachment permit.

“System-Level Sharing” means any automated, recurring, bulk, network, portal, database, vendor-platform, or default sharing configuration that allows another agency, jurisdiction, vendor, system, fusion center, or third party to access ALPR Data without a separate case-specific request and DPS approval.

3. Approved Deployment

The approved deployment is described in Exhibit A.

DPS will not approve, support, recommend, or provide a no-objection response for any Agency-procured ALPR deployment on or near state highway or interstate highway right-of-way unless:

- A.** DPS approves the operational purpose, location, camera number, camera orientation, field of view, deployment justification, and public-safety need;
- B.** Agency has executed this Agreement or another DPS-approved written agreement;
- C.** Agency has obtained, or agrees to obtain and maintain, an ADOT encroachment permit;
- D.** Agency’s vendor contract, purchase order, subscription agreement, data-processing agreement, or other contracting vehicle contains DPS-approved terms sufficient to satisfy this Agreement;
- E.** the ALPR system is configured to provide DPS complete, continuing, and timely access to ALPR Data and audit information;
- F.** DPS determines that the deployment is consistent with law, DPS policy, public-safety needs, privacy considerations, cybersecurity requirements, statewide ALPR governance standards, and where applicable, an ADOT encroachment permit has been obtained, or will be obtained, by the Agency; and
- G.** Agency agrees that DPS may require modification, suspension, relocation, deactivation, removal, or termination of the deployment or Agency access as provided in this Agreement or in accordance with the terms of any ADOT encroachment permit obtained by Agency.

No ALPR equipment may be installed, activated, connected, accessed, or used on or near state highway or interstate highway right-of-way until DPS issues written operational approval and

any required ADOT approval has been obtained by the acquisition of an ADOT encroachment permit.

4. Agency Procurement, Payment, Budget, and Property

Agency is solely responsible for directly procuring and paying for the ALPR equipment, software, subscription, data service, data hosting, installation, maintenance, repair, replacement, utilities, connectivity, removal, and related services covered by this Agreement, unless the Parties expressly agree otherwise in a written amendment.

DPS will not receive Agency funds for this deployment, will not act as a pass-through fiscal agent, and will not be responsible for paying Agency's vendor or reimbursing Agency's costs.

Agency represents that its procurement, funding, vendor contract, and payment mechanism comply with all laws, policies, fiscal controls, and procurement requirements applicable to Agency, and that Agency's vendor agreement does not conflict with this Agreement.

Agency shall not agree to any vendor term, system setting, data-sharing rule, confidentiality term, ownership term, access limitation, audit limitation, retention limitation, export limitation, or public-records/legal-process limitation that conflicts with this Agreement or limits DPS access to ALPR Data.

Each Party is responsible for its own internal budget and costs. Unless otherwise stated in Exhibit B, no funds will be transferred between the Parties. To the extent A.R.S. § 11-952 requires a budget for this undertaking, Exhibit B identifies the manner of financing and maintaining the budget.

Unless otherwise stated in Exhibit B, ALPR equipment procured by Agency remains Agency-owned or vendor-owned property, subject to DPS operational approval, DPS access rights, and the use, sharing, retention, audit, suspension, termination, and removal requirements in this Agreement.

5. DPS Review, Approval, and Continuing Authority

DPS may deny, limit, condition, suspend, withdraw, modify, relocate, deactivate, or require removal of any camera or Agency access if DPS determines that the deployment is not operationally justified, is duplicative, exceeds the approved purpose, creates an unacceptable privacy, cybersecurity, legal, or public-safety risk, conflicts with law or policy, conflicts with the terms of any ADOT encroachment permit obtained for the purpose of installing the ALPR in state highway right of way, is not supported by required approvals, or is inconsistent with statewide ALPR governance.

DPS approval is continuing and conditional. Agency's installation, operation, access, and data sharing remain subject to DPS review, DPS audit, DPS security requirements, DPS access requirements, and DPS written directives issued under this Agreement.

Agency shall not materially modify camera location, mounting, field of view, orientation, retention, sharing, access settings, vendor integration, hot-list integration, or data export settings without prior written DPS approval and applicable ADOT encroachment permit.

6. Authorized Use and Access - Criminal Justice Use Only

Agency and its authorized users may access, query, use, export, disclose, or share ALPR Data only: (a) for the Administration of Criminal Justice and under the same use limitations that apply to CJIS/ACJIS access criteria, including a legitimate criminal justice purpose supported by an Agency responsibility; or (b) for a documented and authorized internal administrative investigation of alleged employee misconduct, when the use is narrowly tailored to the allegations, supported by articulable facts, assigned a trackable internal-affairs or other Agency investigation number, and conducted in accordance with applicable law and Agency policy.

Each user-initiated, individualized manual query of stored ALPR Data must be supported by a trackable criminal case number, incident number, alert number, internal-affairs case number, or other DPS-approved tracking number sufficient to allow later audit of the authorized purpose. This requirement does not apply to automated plate reads, automated hot-list comparisons, system-generated alerts, or other automated system functions occurring without a user-initiated search.

Agency shall ensure that each authorized user has unique credentials, holds and maintains current ACJIS Terminal Operator Certification (“TOC”) as a condition of access, and accesses ALPR Data only through a DPS-approved system.

Agency shall not use ALPR Data for personal, political, commercial, civil-code, debt-collection, private repossession, routine or generalized employee-monitoring, generalized surveillance, non-criminal-justice, or public-records-request purposes. Notwithstanding the foregoing, Agency may use ALPR Data in a documented internal administrative or criminal investigation of alleged employee misconduct when the use is narrowly tailored to the alleged misconduct, supported by articulable facts, assigned a trackable internal-affairs, criminal case, incident, or other approved investigation number, and authorized in accordance with Agency policy.

Agency shall not use ALPR Data for general traffic enforcement unless expressly authorized by law and DPS policy.

Agency shall not sell, exchange, disclose, export, download, screenshot, copy, print, externally store, or otherwise share ALPR Data except as expressly authorized by DPS, this Agreement, and applicable law.

7. DPS Access Must Not Be Limited

Agency shall not restrict, delay, disable, condition, or otherwise limit DPS access to ALPR Data, audit logs, system records, vendor records, exports, reports, alert information, retention

settings, sharing settings, user lists, or other information necessary for DPS to review, audit, use, preserve, disclose, or govern the ALPR system.

Agency shall ensure that DPS has complete, continuing, and timely administrative and law-enforcement access to ALPR Data generated by the approved deployment, including access needed for criminal investigations, public-records review, legal process, litigation holds, audit, compliance review, security review, and statewide ALPR governance.

Agency shall not, and shall not instruct, authorize, or permit any vendor or other third party to, deny, delay, condition, restrict, charge DPS for, or otherwise interfere with DPS access required by this Agreement. At its sole cost, Agency shall provide or cause its vendor to provide all user accounts, licenses, interfaces, application programming interfaces, integrations, connectivity, technical support, and other capabilities reasonably necessary for DPS to obtain and maintain the access required by this Agreement.

Any proprietary, contractual, financial, or technical limitation that prevents or materially impairs DPS access required by this Agreement is a material compliance issue and must be corrected by Agency at Agency's sole expense unless DPS agrees otherwise in writing.

8. Data Sharing, Approved Participating Agencies, and No Out-of-State Sharing

Agency authorizes DPS to make ALPR Data from the approved deployment available to other Approved Participating Agencies that have entered or completed the same DPS-approved ALPR agreement or system MOU and, where applicable, the ADOT permitting process and criteria required for their deployment.

Agency will be provided with access to ALPR Data made available by other Approved Participating Agencies under the same reciprocal terms, subject to DPS approval, system capability, vendor limitations accepted by DPS, law, policy, audit requirements, and the operational needs of DPS and the participating agencies.

Agency shall not engage in System-Level Sharing of ALPR Data with any federal agency, out-of-state agency, out-of-state system, foreign agency, private entity, commercial entity, or non-law-enforcement entity unless DPS determines that the sharing is appropriate and authorizes it through a separate DPS-approved system MOU, data-sharing agreement, or written authorization.

Agency shall not permit default vendor-network sharing, national sharing, multi-state sharing, or vendor-enabled third-party access unless expressly approved by DPS in writing.

Nothing in this section prohibits a disclosure required by valid legal process after notice to DPS, or a case-specific disclosure expressly approved by DPS and permitted by law.

9. Logs, Audits, Retention, and Legal Process

Each user-initiated query, user access, alert review, export, disclosure, and sharing event must be logged in a secure audit system that records, as applicable, the user, date, time, purpose,

tracking number, search terms, results, export, disclosure, and recipient agency if shared. Automated plate reads, automated hot-list comparisons, and system-generated alerts must be logged to the extent supported by the system but need not include a case, incident, or investigation number unless a user accesses, reviews, queries, or acts upon the automated event.

Agency shall not disable, bypass, alter, purge, or interfere with audit logging.

Agency shall conduct or cooperate with audits required by DPS. DPS may audit Agency's ALPR access, TOC certification and user-access eligibility, queries, documentation, user lists, legal-process responses, exports, vendor compliance, retention practices, and security controls at any time.

ALPR Data not associated with a hit, alert, case, or legal hold shall be purged automatically at the end of the retention period stated in Exhibit A. Agency shall configure the system to purge automatically and shall not extend the retention period without prior written DPS approval. All other ALPR Data shall be retained and destroyed according to the records-retention schedule applicable to Agency under A.R.S. §§ 41-151.15 and 41-151.19, litigation holds, criminal-investigation preservation requirements, and applicable law.

Agency shall immediately notify DPS of any public-records request, subpoena, discovery request, court order, warrant, litigation hold, preservation request, media request, or other legal demand seeking ALPR Data or records related to the ALPR system.

Agency shall consult with DPS before releasing ALPR Data or related system records. Nothing in this Agreement requires Agency to violate a lawful public-records, discovery, or court obligation, but Agency shall provide DPS a reasonable opportunity to review and assert any applicable privilege, confidentiality, privacy, security, law-enforcement, or best-interests-of-the-State basis before release when legally permissible.

10. Verification Before Enforcement Action

When practicable, before taking enforcement action based solely on an ALPR alert, Agency personnel shall verify the alert through an authorized law-enforcement database, dispatch confirmation, or another DPS-approved verification method.

An ALPR alert alone does not establish probable cause or reasonable suspicion unless supported by the totality of the circumstances and applicable law.

11. Vendor Requirements

Agency shall ensure that any vendor used for ALPR equipment, software, storage, installation, maintenance, cloud hosting, transmission, analytics, data processing, subscription services, or related services is contractually required to comply with this Agreement.

Agency's vendor agreement must prohibit sale, exchange, marketing use, commercial use, unauthorized disclosure, independent use, or third-party sharing of ALPR Data. It must also include DPS-approved terms addressing data ownership or control, full and complete DPS

access, confidentiality, cybersecurity, breach notification, audit logs, user permissions, export controls, retention, deletion, public records, legal process, subcontractors, and termination assistance.

Agency's vendor agreement shall include the provision required by A.R.S. § 44-7953 prohibiting the vendor from selling or disseminating to any third party any data collected by the ALPR system. Agency shall certify in writing to DPS that this provision is included before DPS issues written operational approval.

Agency's vendor agreement shall expressly require the vendor to provide, at no cost to DPS or ADOT, all access, licenses, interfaces, integrations, connectivity, technical support, records, and other capabilities required by Sections 7 and 12. The vendor shall not require DPS or ADOT to enter into a separate agreement, purchase a license or subscription, accept additional vendor terms, or pay any fee as a condition of receiving the access required by this Agreement.

Agency shall provide DPS with a copy of any vendor agreement, order, statement of work, data-processing agreement, subscription agreement, privacy policy, data-sharing configuration, retention configuration, or system setting relevant to this deployment upon request.

Agency has no authority to direct a DPS system, DPS user, or DPS statewide ALPR governance process. Agency shall communicate requested changes, concerns, or operational needs to DPS, and DPS shall determine whether to approve or implement them.

12. ADOT Permit Compliance

Agency shall obtain, maintain, and comply with all ADOT permits, right-of-way approvals, utility approvals, location requirements, safety requirements, installation requirements, maintenance requirements, removal requirements, and other permit-related criteria applicable to the approved deployment.

At Agency's sole cost, Agency shall provide or cause its vendor to provide ADOT reasonable access to the physical ALPR equipment, camera installations, mounting and utility infrastructure, maintenance and repair records, system-status information, and other non-ALPR Data reasonably necessary for ADOT to administer, inspect, enforce, or verify compliance with an applicable permit or right-of-way requirement.

Nothing in this paragraph authorizes ADOT to query the ALPR system, access ALPR Data, or receive criminal-investigative or other law-enforcement information unless such access is separately authorized by law and approved in writing by DPS.

Agency's failure to meet, comply with, or maintain any applicable ADOT encroachment permit, right-of-way condition, or ADOT/DPS permit-related directive constitutes a violation of this Agreement and may result in immediate suspension, deactivation, removal, termination, or withdrawal of DPS approval or no-objection.

Agency shall immediately notify DPS of any ADOT concern, permit deficiency, notice of violation, request for modification, safety issue, maintenance issue, or other issue affecting the approved deployment.

13. Change in Law / No DPS Liability for Loss of Access

Agency acknowledges that ALPR access, sharing, retention, disclosure, and system operation are subject to changes in federal law, Arizona law, court orders, Attorney General guidance, DPS policy, ADOT requirements, procurement requirements, vendor terms, cybersecurity requirements, and statewide ALPR governance standards.

DPS may immediately suspend, limit, modify, condition, or terminate Agency's access to ALPR Data or use of any ALPR system if DPS determines that continued access or use may violate law, conflict with policy, create unacceptable risk, or conflict with the terms of any ADOT encroachment permit obtained for the purpose of installing the ALPR in state highway right of way or statewide governance requirements.

Agency assumes the risk that future law, policy, court decisions, permit requirements, vendor limitations, or funding restrictions may limit, reduce, suspend, or eliminate Agency's access to ALPR Data or continued operation of the deployment.

To the fullest extent permitted by law, DPS shall not be liable to Agency for damages, reimbursement, reliance costs, lost grant funds, vendor charges, subscription charges, equipment costs, installation costs, removal costs, operational costs, or other costs arising from DPS's lawful suspension, limitation, modification, relocation, deactivation, removal, or termination of a deployment or access under this Agreement.

14. Security Incidents and Misuse

Agency shall notify the DPS Highway Patrol Division Assistant Director or designee and the DPS-designated information-security incident contact immediately, and in no event later than one hour after discovery, of any suspected or confirmed unauthorized access, improper query, unauthorized disclosure, credential compromise, cybersecurity incident, vendor incident, material audit anomaly, material error, misuse, or other event that may affect ALPR Data or system integrity.

Agency and its vendor shall promptly provide DPS all information reasonably requested and legally permitted to assess, investigate, contain, remediate, and document the incident, including relevant reports, ALPR Data, audit logs, security logs, vendor records, communications, and investigative findings.

Agency and its vendor shall preserve all relevant logs, records, communications, exports, ALPR Data, and other evidence relating to the incident. Agency and its vendor shall not alter, delete, overwrite, or destroy such information except as authorized in writing by DPS or required by law.

For any suspected or confirmed cybersecurity or privacy incident affecting ALPR Data or system integrity, DPS shall promptly notify and coordinate with the Arizona Department of Homeland Security's Arizona Cyber Command. Agency and its vendor shall cooperate with DPS and Arizona Cyber Command and shall timely implement reasonable containment, investigative, remediation, mitigation, and protective measures directed by DPS or required by applicable law or statewide information-security policy.

DPS may immediately suspend any user, Agency access, vendor access, camera, location, or system connection while an incident is investigated. DPS may continue the suspension until DPS, after consultation with Arizona Cyber Command as appropriate, determines that the incident has been contained, required mitigation has been completed, and continued access or operation no longer presents an unacceptable legal, privacy, cybersecurity, operational, or public-safety risk.

15. Insurance and Indemnification

Each Party is responsible for its own acts, omissions, negligence, misconduct, and legal obligations.

Each Party, as Indemnitor, agrees to defend, indemnify, and hold harmless the other Party, as Indemnitee, from claims, losses, liability, costs, or expenses, including reasonable attorneys' fees, arising out of bodily injury of any person, including death, or property damage, but only to the extent such claims result in vicarious or derivative liability to the Indemnitee caused by the act, omission, negligence, misconduct, or other fault of the Indemnitor, its officers, officials, agents, employees, or volunteers.

DPS is self-insured pursuant to A.R.S. § 41-621. Agency shall provide evidence of insurance or self-insurance upon request, unless Agency is a State of Arizona agency for which such requirement is not applicable.

Agency shall require each contractor, subcontractor, and vendor performing installation, maintenance, repair, or removal work under this Agreement to (1) indemnify the State of Arizona, its departments, agencies, boards, commissions, universities, officers, officials, agents, and employees to the same extent it indemnifies Agency, and (2) name the State of Arizona, DPS, and ADOT as additional insureds on its commercial general liability and automobile liability policies. Agency shall also require the insurance limits and terms specified by Agency procurement requirements, applicable State Risk Management requirements, and any ADOT encroachment permit. Agency shall not require DPS to indemnify Agency, any vendor, ADOT, or any other person or entity.

16. Term, Termination, and Disposition

This Agreement becomes effective on the later of the date of final signature or the date each Party has taken the action required by A.R.S. § 11-952(A) and (F) to authorize it, and remains in effect until _____, unless terminated earlier. Agency represents that its governing body has authorized this Agreement by ordinance, resolution, or other action required by law, and shall provide DPS a copy of that action on request.

DPS may suspend or terminate this Agreement, in whole or in part, immediately upon written notice if DPS determines that continued access or operation may violate law, Agency or vendor has misused ALPR Data, Agency or vendor has failed to comply with this Agreement, Agency has failed to maintain any required ADOT encroachment permit or requirements, or continued operation creates unacceptable legal, privacy, cybersecurity, operational, fiscal, or public-safety risk.

Either Party may terminate this Agreement for convenience upon 30 days' written notice, subject to lawful costs incurred before termination and subject to legal preservation requirements, the terms of any required ADOT encroachment permit, and removal or closeout obligations.

Upon termination, Agency shall stop using ALPR Data, terminate or modify user access as directed by DPS, preserve records subject to legal hold, and return or destroy ALPR Data as directed by DPS and allowed by law.

Property disposition shall be governed by Exhibit B and applicable ADOT encroachment permit requirements. Agency is responsible for removal, restoration, and closeout costs unless DPS agrees otherwise in writing.

17. Required State Terms

This Agreement is subject to cancellation pursuant to A.R.S. § 38-511.

The Parties agree to resolve disputes arising out of or relating to this Agreement through arbitration after exhausting applicable administrative review, to the extent required by A.R.S. § 12-1518.

The Parties and any vendor shall comply with applicable federal and state nondiscrimination laws, including applicable requirements of State Executive Order 2023-001 and the Americans with Disabilities Act.

If applicable, Agency shall ensure that any vendor used by Agency for this deployment complies with A.R.S. §§ 41-4401 and 23-214 and all federal, state, and local immigration laws and regulations.

Unless specifically approved in writing by DPS and permitted by law, any services involving access to secure, sensitive, confidential, law-enforcement, or personal data shall be performed within the United States.

This Agreement may be amended only by written amendment signed by authorized representatives of both Parties and approved as required by law.

DPS may issue written operational, security, access, audit, retention, or compliance directives without a formal amendment if the directive does not materially change the funding obligation or duration of the Agreement.

If any provision is held invalid or unenforceable, the remaining provisions fully remain in effect permitted by law.

Except for the Arizona Department of Transportation, which is an intended third-party beneficiary of Sections 11 and 12 solely as to the access and no-cost provisions expressly running in its favor, this Agreement creates no third-party beneficiaries.

This Agreement, including Exhibits A and B, is the entire agreement between the Parties regarding Agency's ALPR deployment, access, sharing, and data governance on or near state highway or interstate highway right-of-way.

18. Notices

Notices under this Agreement shall be sent to:

For DPS:

Arizona Department of Public Safety

DPS may designate or update its operational, information-security, and incident-response contacts by written notice to Agency without a formal amendment to this Agreement. Notifications required by Section 14 shall be made using the then-current contact information designated by DPS and shall not be delayed by the formal-notice requirements applicable to other notices under this Agreement.

For Agency:

19. Attorney Approval and Signatures

In accordance with A.R.S. § 11-952, this Agreement shall be submitted to the attorney for each Party before execution. Each attorney shall determine whether the Agreement is in proper form and within the powers and authority granted to the Party under Arizona law.

Arizona Department of Public Safety

By: _____

Name: _____

Title: _____

Date: _____

Approved as to Form and Authority:

By: _____

Name: _____

Title: _____

Date: _____

By: _____

Name: _____

Title: _____

Date: _____

Approved as to Form and Authority:

By: _____

Name: _____

Title: _____

Date: _____

Exhibit A

This Exhibit A identifies the Agency-procured ALPR deployment approved under the Agreement.

Item	Description
Requesting Agency	
DPS Program Contact	
Agency Contact	
Vendor / System	
ADOT Permit / Application Number	
Approved Deployment Term	
Approved Retention Period	

Approved Location(s)

Field	Description
Camera ID	
Roadway / Route	
Milepost / Cross Street	
GPS Coordinates	
Direction / Field of View	
Mounting / Power / Connectivity	
ADOT Permit Condition(s)	
DPS Approval Notes	

Approved Operational Purpose

The approved criminal justice purpose for this deployment is:

Agency may not use this deployment for any purpose not authorized by the Agreement or approved by DPS in writing.

No change to camera number, location, orientation, field of view, vendor integration, access setting, retention setting, sharing setting, or hot-list integration is approved unless DPS approves the change in writing.

Exhibit B

This Exhibit B identifies the funding, budget, cost allocation, and property-disposition terms for the Agency-procured ALPR deployment.

No Pass-Through Funding

Unless expressly amended in writing, Agency will directly procure and pay for all ALPR equipment, software, subscriptions, data services, installation, maintenance, repair, replacement, utilities, connectivity, removal, and related services. No funds will be paid to DPS for pass-through to a vendor.

Budget and Cost Allocation

Cost Category	Responsible Party	Funding Source / Payment Method	Notes
Equipment / procurement	Agency		
Installation	Agency		
Subscription / licensing / data hosting	Agency		
Required DPS/ADOT access, licenses, interfaces, integrations, connectivity, and technical support	Agency		
Maintenance / repair / replacement	Agency		
Utilities / connectivity	Agency		
Removal / restoration / closeout	Agency		
DPS administrative review / audit / governance	DPS		

Agency certifies that the identified funds are legally available for the approved purpose and may be used in a manner that allows Agency and its vendor to comply with DPS access, data governance, sharing, retention, audit, suspension, termination, removal, and use limitations required by the Agreement.

DPS has no obligation to expend funds not appropriated, allocated, encumbered, or legally available, and no obligation to reimburse Agency for any cost incurred under or related to this Agreement.

Property Disposition

Property / Item	Ownership or Control	Disposition Upon Termination
ALPR camera equipment		
Mounting / power / communications equipment		
ALPR Data	Subject to DPS access and data-governance requirements	Retain or destroy under DPS-approved retention requirements, legal holds, and applicable law
Vendor account / portal / access	Agency/vendor account subject to DPS access requirements	Terminate, modify, or preserve as directed by DPS and allowed by law