

Project Overview & Scope of Work

The following definitions and links are used throughout the RFP.

County: Dane County

County Agency: Department/Division utilizing the service or product.

Dane County Purchasing website: <https://www.danepurchasing.com/>

Proposer/Vendor/Firm/Contractor: a company submitting a proposal in response to this RFP.

Purpose

1. The Dane County Sheriff's Office (DCSO) is soliciting proposals from qualified vendors to provide a comprehensive Automated License Plate Reader (ALPR) system including fixed infrastructure cameras, cloud-based data management, and integration with existing agency cloud software platforms. The system must satisfy DCSO's privacy, civil liberties, data governance, and public accountability requirements.
2. This RFP is intended to identify a vendor capable of delivering a modern, scalable, and fully integrated ALPR solution that advances DCSO's public safety mission.

Background

1. DCSO currently operates a suite of public safety technologies. The agency seeks an ALPR solution that complements its existing investments and operates within a unified, cloud-based evidence and data ecosystem.
2. The selected vendor must demonstrate the ability to integrate natively and securely with the agency's existing platforms without requiring duplicate infrastructure, separate portals or redundant data stores.
3. The County Board has authorized funding of up to \$80,000 annually for this program. Proposers shall clearly identify all one-time and recurring fees.
4. Requirements throughout this RFP reflect those conditions. Vendors must be prepared to address these requirements in full.

Community & Board Priorities

The following priorities are foundational to this procurement and are reflected in the mandatory requirements of this RFP:

1. Vendor shall provide proof of independent third-party auditing of their system's privacy and security protections with public disclosure of findings.
2. Exclusive ownership, control, and management of all collected data by DCSO
3. Detailed public reporting on data access to ensure no unauthorized third-party rights
4. Strict data retention limits and clearly defined automated deletion policies

5. Restricted, role-based user access controls with comprehensive audit logging.
6. Prohibition on unauthorized data sharing, sale or external access.
7. Strict limitations on collection and retention of non-license plate imagery
8. Full compliance with applicable local, state, and federal laws
9. Public transparency measures, including DCSO's ability to publish a public-facing data use policy.
10. No facial recognition capabilities of any kind.
11. AI use limited strictly to license plate character recognition and basic vehicle attribute identification.

Scope of Work/Specifications

The selected vendor shall furnish all labor, equipment, software, subscriptions, implementation services, integrations, documentation, support, and other deliverables necessary to provide a fully functional ALPR solution meeting the requirements of this RFP. At a minimum, the scope shall include:

1. Supply and installation of fixed ALPR camera infrastructure at locations designated by DCSO.
2. Cloud based ALPR data platform with real-time and historical query capabilities.
3. Integration capabilities with DCSO's existing public safety technologies.
4. Mobile application access for field personnel.
5. System training, ongoing technical support, and warranty coverage.
6. Public facing transparency portal enabling DCSO to publish its data governance and usage policies. Project management, implementation planning, testing, and acceptance support.
7. Transition-out assistance and data return at contract end.

Vendor Qualifications

MANDATORY QUALIFICATIONS:

1. The vendor shall have a minimum of five (5) years of experience providing ALPR solutions to US law enforcement agencies.
2. The vendor shall maintain a US based customer support operation staffed 24/7/365.
3. The vendor shall provide a minimum of three (3) reference agencies with deployments comparable in scale to DCSO that are using both the vendor's ALPR system and the vendor's digital evidence management platform simultaneously.
4. The vendor shall maintain a current SOC 2 Type II report, and current ISO/IEC 27001, and ISO/IEC 27701 certifications, and shall provide documentation at proposal submission.

5. The vendor shall demonstrate current CJIS compliance via a signed CJIS Security Addendum or equivalent documentation.

Training & On-Going Support

MANDATORY REQUIREMENTS:

1. The vendor shall provide comprehensive initial training for DCSO administrators, investigators, and patrol personnel. Training shall be role-appropriate and cover both technical operation and DCSO's policy and governance responsibilities.
2. The vendor shall support a train-the-trainer model enabling DCSO training leads to certify new personnel internally, including new deputies joining patrol.
3. On-demand online training modules shall be available for both patrol and administrative roles, ensuring new personnel can complete required training without waiting for scheduled sessions.
4. The vendor shall provide 24/7/365 technical support staffed by U.S.-based personnel.
5. The vendor shall assign a dedicated customer success representative to DCSO for the duration of the contract.

Implementation Plan

Vendor shall submit a detailed implementation plan including:

1. Project governance
2. Project schedule
3. Staffing and responsibilities
4. Installation approach
5. Integration steps
6. Training plan
7. Testing plan
8. Go-Live Plan
9. Post Go-Live support approach

Warranty, Maintenance & Product Support

Vendor shall state the warranty period for camera hardware, accessories, installation workmanship, and software defects.

Vendor shall identify:

1. Replacement process

2. Advance replacement options
3. Firmware update practices
4. Security patch practices
5. End-of-life notice period
6. Spare parts/support availability
7. Any exclusions

Hardware Requirements - Fixed ALPR Camera Infrastructure

MANDATORY REQUIREMENTS:

1. DCSO anticipates an initial deployment of twenty-six (26) fixed ALPR cameras. Final quantities and locations shall be determined by DCSO based on project needs and available funding.
2. Cameras shall be purpose-built for law enforcement ALPR application with all-weather IP66 or higher rated enclosures.
3. Cameras shall capture front and/or rear plates at vehicle speeds of 0-100 mph with no manual focusing required.
4. Cameras shall operate effectively in low-light and nighttime conditions using IR illumination.
5. The system shall provide real-time data transmission to a cloud-based platform with latency under three (3) seconds from capture to alert.
6. The hardware shall be manufactured and assembled by the vendor to ensure clear and transparent customer support; third party rebranded hardware is not acceptable.
7. The vendor shall offer flexible mounting options including dedicated fixed pole, or mounting to existing county-owned infrastructure.
8. Cameras should support solar/battery power options for off-grid deployment locations.
9. The legal title of LPR camera hardware shall be granted to DCSO upon contract start date.
10. Vendor shall provide a minimum three-year warranty on camera hardware and installation workmanship, including advance replacement of failed hardware when feasible-and/or coverage for vandalism and accidents, as well as no-cost firmware/security updates for the supported life of the product.

Software Platform & Cloud Architecture

MANDATORY REQUIREMENTS:

1. The data platform shall be entirely cloud-hosted with no requirement for on-premises servers at DCSO facilities.

2. The platform shall provide a web-based investigative portal accessible without installing client-side software.
3. The system shall support real-time hot list alerts delivered to in-car and mobile devices within three (3) seconds of a plate read matching alert criteria.
4. The platform shall support historical plate queries with date/time, location, and vehicle attribute filters.
5. The platform shall support targeted, location-based alerting capabilities that allow authorized personnel to define specific geographic zones and receive notifications regarding specific vehicles of interest entering or exiting those zones. All searches are subject to existing policies, legal requirements, audit logging, data retention and oversight controls.
6. All LPR data shall be stored within a CJIS authorized cloud infrastructure with data residency within the United States.
7. The platform shall maintain a complete, immutable audit log of all user queries, exports, and data access events. Audit logs shall have an infinite retention period and shall not be able to be deleted by any user, including agency administrators.
8. The vendor's platform shall comply with FBI CJIS Security Policy requirements. The vendor shall provide a current CJIS compliance attestation and evidence of CJIS security training for all personnel with access to agency data.
9. The platform shall hold a valid SOC 2 report. Documentation shall be provided at proposal submission.
10. The vendor shall hold current ISO/IEC 27001:2022 & ISO/IEC 27701:2019 certifications. Documentation shall be provided at proposal submission.
11. The vendor shall publish a publicly accessible trust and compliance portal documenting all current security and privacy certifications.
12. The proposed solution shall support authentication and identity management through Microsoft Entra ID using industry-standard protocols (e.g., SAML 2.0 and/or OpenID Connect), enabling centralized user provisioning, authentication, and role-based access control.

Data Security & Incident Response

MANDATORY REQUIREMENTS:

1. Vendor shall notify DCSO of any actual or suspected security incident involving DCSO data immediately, and in no event later than twenty-four (24) hours after discovery.
2. Vendor shall provide ongoing incident updates, root cause analysis, corrective actions, and full cooperation with DCSO's incident response, legal, audit, and public communication obligations.

Platform Integration with Existing Agency Public Safety Technology Platforms

MANDATORY REQUIREMENTS:

1. The ALPR platform shall natively integrate with DCSO's existing digital evidence management system (DEMS), enabling LPR reads and associated images to be directly linked to DEMS cases without manual export/import.
2. Officers shall be able to access ALPR search results and receive real-time alerts through the same mobile applications used for existing body-worn camera and in-car video review.
3. The ALPR platform shall support evidence sharing and collaboration features consistent with the agency's existing DEMS, including chain of custody tracking for LPR exports.
4. The vendor shall demonstrate a documented integration with the agency's existing platforms at the time of proposal submission, including reference agencies using both systems simultaneously.
5. The ALPR data shall be accessible within the same investigative timeline view used for body-worn camera footage, in-car video, and other digital evidence.
6. The vendor should support integration with certified third-party cameras, including commercial cameras voluntarily shared with DCSO, through a managed partner program. All such integrations shall be agency-controlled and auditable.

Mobile & Field Access

MANDATORY REQUIREMENTS:

1. The vendor shall provide a native iOS mobile application for field access to ALPR data, real-time alerts and manual plate queries.
2. The mobile application shall function as part of the vendor's unified public safety platform, not as a stand-alone ALPR-only application.
3. Real-time hot-list alerts shall be delivered as push notifications to officer mobile devices with plate image, vehicle description, and alert reason.
4. Officers shall be able to conduct manual plate queries from the mobile applications while offline in degraded network conditions, with results syncing upon reconnection.

Privacy, Data Governance & Community Accountability

MANDATORY REQUIREMENTS:

1. The DCSO shall retain full, exclusive ownership of all ALPR data collected through the system. The vendor shall not pool, aggregate, resell, or repurpose agency data for any commercial,

analytical, or law enforcement purpose outside of delivering the contracted service to DCO. This shall be a contractual commitment, not solely a policy statement.

2. The vendor shall not provide any federal agency, including ICE, DHS, or any other entity, with independent access to DCSO data. Any federal access shall require either valid legal process directed to DCSO or an agency-approved sharing relationship explicitly configured and approved by DCSO administrators
3. The vendor shall not sell, resell, or transfer DCSO ALPR data to any third party under any circumstances without explicit written authorization from DCSO.
4. The platform shall include a public-facing ALPR Policy and Transparency Portal that DCSO can use to publish its retention policies, data sharing posture, usage metrics, and program governance details. DCSO shall have full control over what is published and may enable or disable the portal at any time.
5. The platform shall support configurable, automated data retention policies. Non-evidentiary detections shall be automatically purged when the agency-defined retention period is reached, with no manual deletion required. DCSO shall be able to modify retention periods at any time.
6. The system shall support role-based access controls (RBAC) allowing DCSO administrators to define granular permissions by user, group, and data type. All administrative controls shall be fully auditable.
7. Each detection shall capture only: a license plate image, a vehicle context image, basic vehicle attributes (make, model, color), and time/location metadata. The system shall not capture facial imagery, driver identity information, passenger data, or any personal record beyond the plate and vehicle. Context imagery shall be used solely for vehicle identification purposes.
8. The system shall not share DCSO data with any other law enforcement agency, commercial entity, or government body without an explicit sharing relationship configured and approved by DCSO. All sharing shall use federated access — recipient agencies query authorized data but do not take ownership of it. DCSO retains sole ownership and disclosure authority at all times.
9. The vendor's platform shall comply with all applicable local, state, and federal laws. The vendor shall provide documentation of its compliance framework and shall make available legal and compliance support to assist DCSO in meeting Wisconsin-specific requirements.
10. Reasonable administrative, technical, and physical safeguards must be implemented to protect any personal, confidential, or sensitive data accessed, processed, or stored. At minimum, the following safeguards are required:
 1. Breach Notification
 1. Dane County must be notified of any known or suspected data breach within seventy-two (72) hours of discovery.

2. Access Controls

1. Data access must be restricted to authorized personnel only, with mechanisms in place to prevent unauthorized data exposure.

3. Data Use Prohibition

1. No personal, confidential, or sensitive data will be sold, used, or rented without explicit written authorization from the Dane County.

4. Data Disposal or Return

1. Upon completion or termination of the project/contract, all County data must be securely disposed of or returned to Dane County.

5. Compliance with Laws

1. Vendor must comply with all applicable local, state, and federal privacy laws throughout the duration of the project/contract.

11. The Vendor shall provide documentation upon request to demonstrate compliance with these requirements and shall fully cooperate with any audits or assessments conducted by Dane County to verify adherence to data privacy obligations.

AI Use, Surveillance Limitations & Civil Liberties Protections

MANDATORY REQUIREMENTS:

1. No component of the proposed ALPR system — including cameras, software, firmware, or any AI/ML model — shall have facial recognition capabilities. This requirement applies to all hardware and software proposed, including any optional modules or integrations. Vendors shall provide a written attestation confirming the absence of facial recognition in the proposed solution.
2. The system shall not enable continuous, passive surveillance of individuals. Every alert generated by the system shall require human review before any law enforcement action is taken. The system surfaces information for human decision-making — it does not automate enforcement outcomes.
3. The system shall not enable tracking of individuals based on protected characteristics including race, religion, national origin, political affiliation, or participation in lawful protest or assembly.
4. All system activity shall be tied to an authenticated user identity and logged with a timestamp. It shall be technically impossible for any user to conduct ALPR queries or access system data anonymously or without a reviewable audit record.